Name: Rucha Nargunde
UID:2018130032
Batch:C

Experiment 2

AIM : To study basic network utilities

This lab introduces some basic network monitoring/analysis tools. There are a few exercises along the way. You should write up answers to the **ping** and **traceroute** exercises and turn them in next lab. (You should try out each tool, whether it is needed for an exercise or not!).

Prerequisite: Basic understanding of command line utilities of Linux Operating system.

Some Basic command line Networking utilities

Start with a few of the most basic command line tools. These commands are available on Unix, including Linux (and the first two, at least, are also for Windows). Some parameters or options might differ on different operating systems. Remember that you can use man <command> to get information about a command and its options.

ping — The command ping <host> sends a series of packets and expects to receieve a response to each packet. When a return packet is received, ping reports the round trip time (the time between sending the packet and receiving the response). Some routers and firewalls block ping requests, so you might get no reponse at all. Ping can be used to check whether a computer is up and running, to measure network delay time, and to check for dropped packets indicating network congestion. Note that <host> can be either a domain name or an IP address. By default, ping will send a packet every second indefinitely; stop it with Control-C

Network latency, specifically round trip time (RTT), can be measured using ping, which sends ICMP packets. The syntax for the command in Linux or Mac OS is:

```
ping [-c <count>] [-s <packetsize>] <hostname>
```

The syntax in Windows is:

```
ping [-n <count>] [-l <packetsize>] <hostname>
```

The default number of ICMP packets to send is either infinite (in Linux and Mac OS) or 4 (in Windows). The default packet size is either 64 bytes (in Linux) or 32 bytes (in Windows). You can specify either a hostname (e.g., spit.ac.in) or an IP address.

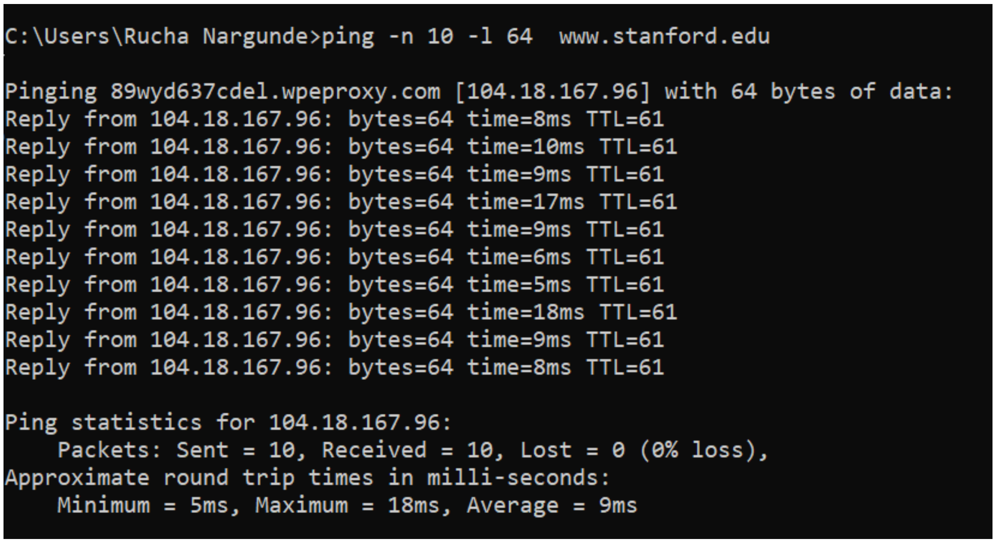
To save the output from ping to a file, include a greater than symbol and a file name at the end of the command. For example:

```
ping -c 10 google.com > ping_c10_s64_google.log
```

Experiments with Ping

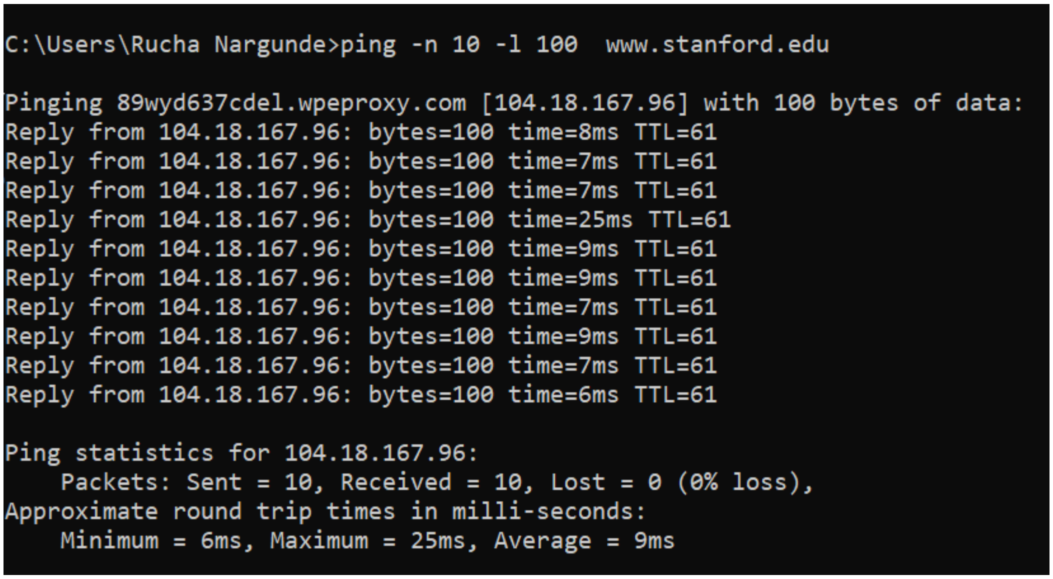
1. Ping the any hosts 10 times (i.e., packet count is 10) with a packet size of 64 bytes, 100 bytes, 500 bytes, 1000 bytes, 1400 bytes

   Pinging www.stanford.edu 10 times with a packet size of 64 bytes



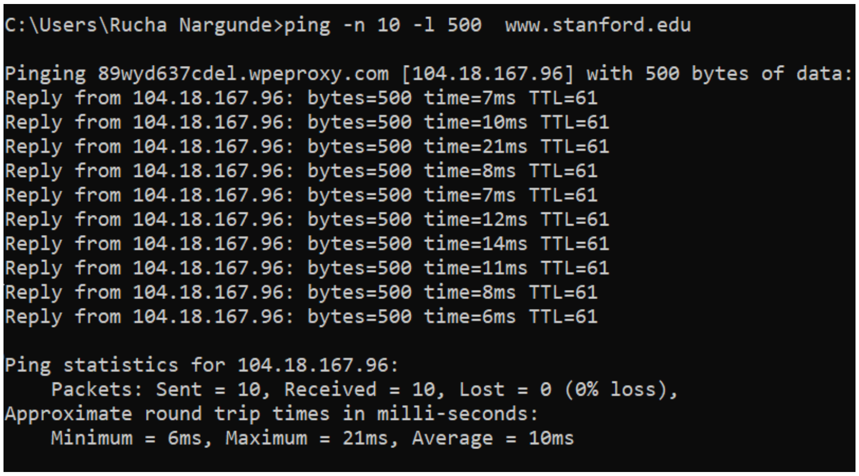
```
C:\Users\Rucha Nargunde>ping -n 10 -l 64  www.stanford.edu

Pinging 89wyd637cdel.wpeproxy.com [104.18.167.96] with 64 bytes of data:
Reply from 104.18.167.96: bytes=64 time=8ms TTL=61
Reply from 104.18.167.96: bytes=64 time=10ms TTL=61
Reply from 104.18.167.96: bytes=64 time=9ms TTL=61
Reply from 104.18.167.96: bytes=64 time=17ms TTL=61
Reply from 104.18.167.96: bytes=64 time=9ms TTL=61
Reply from 104.18.167.96: bytes=64 time=6ms TTL=61
Reply from 104.18.167.96: bytes=64 time=5ms TTL=61
Reply from 104.18.167.96: bytes=64 time=18ms TTL=61
Reply from 104.18.167.96: bytes=64 time=9ms TTL=61
Reply from 104.18.167.96: bytes=64 time=8ms TTL=61

Ping statistics for 104.18.167.96:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 18ms, Average = 9ms
```

   Pinging www.stanford.edu 10 times with a packet size of 100 bytes



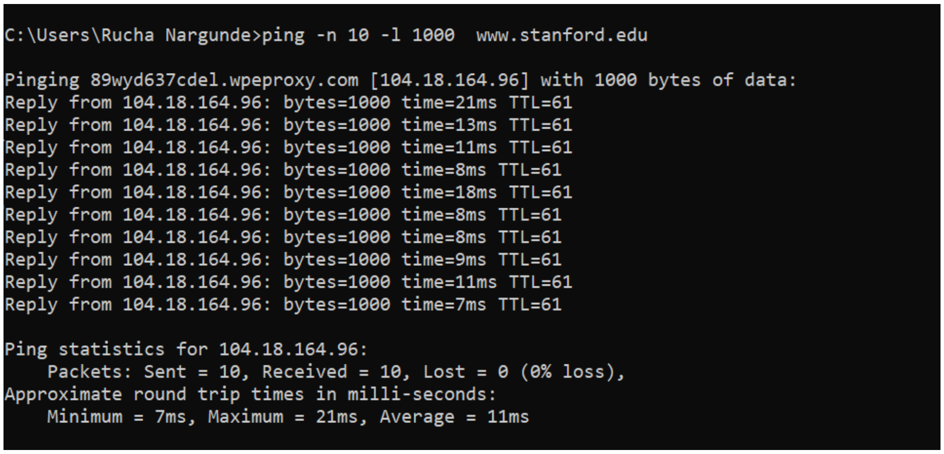
```
C:\Users\Rucha Nargunde>ping -n 10 -l 100  www.stanford.edu

Pinging 89wyd637cdel.wpeproxy.com [104.18.167.96] with 100 bytes of data:
Reply from 104.18.167.96: bytes=100 time=8ms TTL=61
Reply from 104.18.167.96: bytes=100 time=7ms TTL=61
Reply from 104.18.167.96: bytes=100 time=7ms TTL=61
Reply from 104.18.167.96: bytes=100 time=25ms TTL=61
Reply from 104.18.167.96: bytes=100 time=9ms TTL=61
Reply from 104.18.167.96: bytes=100 time=9ms TTL=61
Reply from 104.18.167.96: bytes=100 time=7ms TTL=61
Reply from 104.18.167.96: bytes=100 time=9ms TTL=61
Reply from 104.18.167.96: bytes=100 time=7ms TTL=61
Reply from 104.18.167.96: bytes=100 time=6ms TTL=61

Ping statistics for 104.18.167.96:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 25ms, Average = 9ms
```

Pinging www.stanford.edu 10 times with a packet size of 500 bytes



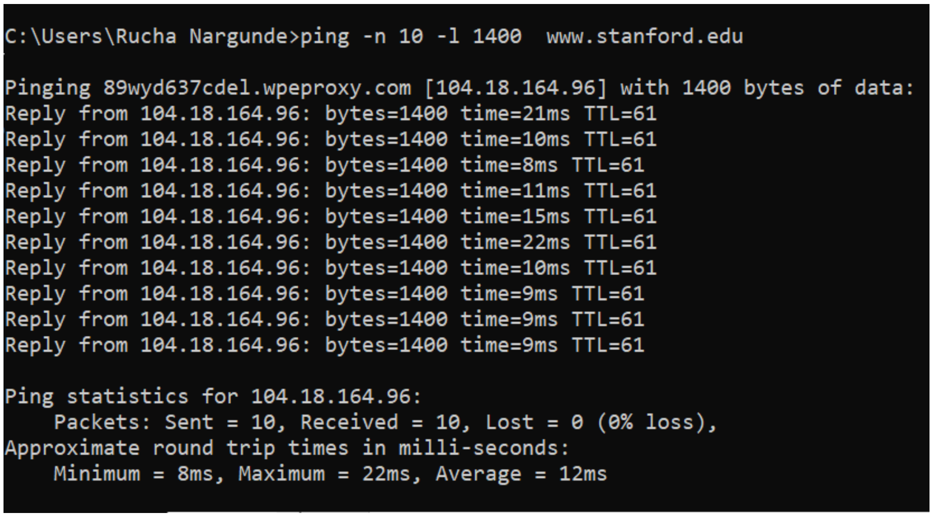
```
C:\Users\Rucha Nargunde>ping -n 10 -l 500  www.stanford.edu

Pinging 89wyd637cdel.wpeproxy.com [104.18.167.96] with 500 bytes of data:
Reply from 104.18.167.96: bytes=500 time=7ms TTL=61
Reply from 104.18.167.96: bytes=500 time=10ms TTL=61
Reply from 104.18.167.96: bytes=500 time=21ms TTL=61
Reply from 104.18.167.96: bytes=500 time=8ms TTL=61
Reply from 104.18.167.96: bytes=500 time=7ms TTL=61
Reply from 104.18.167.96: bytes=500 time=12ms TTL=61
Reply from 104.18.167.96: bytes=500 time=14ms TTL=61
Reply from 104.18.167.96: bytes=500 time=11ms TTL=61
Reply from 104.18.167.96: bytes=500 time=8ms TTL=61
Reply from 104.18.167.96: bytes=500 time=6ms TTL=61

Ping statistics for 104.18.167.96:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 21ms, Average = 10ms
```

Pinging www.stanford.edu 10 times with a packet size of 1000 bytes



```
C:\Users\Rucha Nargunde>ping -n 10 -l 1000  www.stanford.edu

Pinging 89wyd637cdel.wpeproxy.com [104.18.164.96] with 1000 bytes of data:
Reply from 104.18.164.96: bytes=1000 time=21ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=13ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=11ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=8ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=18ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=8ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=8ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=9ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=11ms TTL=61
Reply from 104.18.164.96: bytes=1000 time=7ms TTL=61

Ping statistics for 104.18.164.96:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 21ms, Average = 11ms
```

Pinging www.stanford.edu 10 times with a packet size of 1400 bytes



```
C:\Users\Rucha Nargunde>ping -n 10 -l 1400  www.stanford.edu

Pinging 89wyd637cdel.wpeproxy.com [104.18.164.96] with 1400 bytes of data:
Reply from 104.18.164.96: bytes=1400 time=21ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=10ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=8ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=11ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=15ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=22ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=10ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=9ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=9ms TTL=61
Reply from 104.18.164.96: bytes=1400 time=9ms TTL=61

Ping statistics for 104.18.164.96:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 22ms, Average = 12ms
```

As shown by the above screenshots, RTT increases with increase in packet size

Request timed out error occurs at some places. This is because the server is not accepting Internet Control Message Protocol (ICMP) traffic.

QUESTIONS ABOUT LATENCY

Now look at the results you gathered and answer the following questions about latency. Store your answers in a file named ping.txt.

1. Does the average RTT vary between different hosts? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

Answer: Average RTT can vary between different hosts due to Processing delay, queuing delay, Transmission delay, and Propagation delay [1]

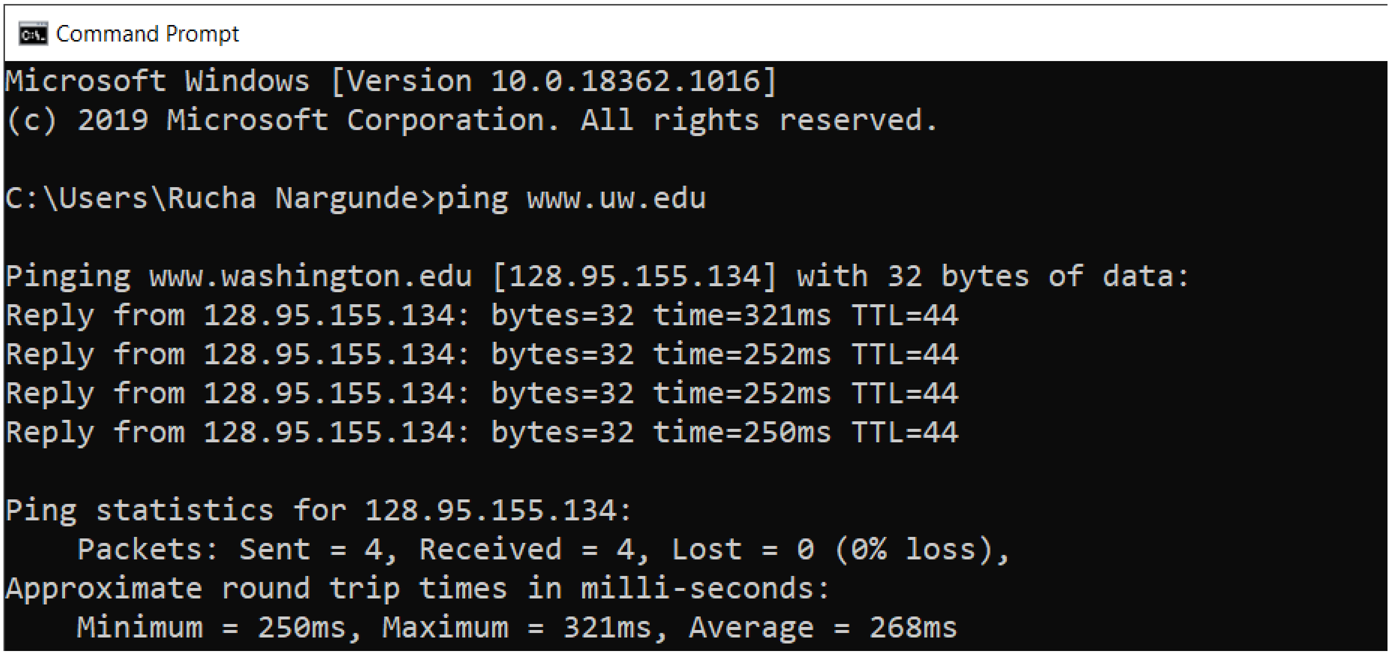
Transmission Delay [1]:
Time taken to put a packet onto link. In other words, it is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network.
Propagation delay [1] :
Time taken by the first bit to travel from sender to receiver end of the link. In other words, it is simply the time required for bits to reach the destination from the start point. Factors on which Propagation delay depends are Distance and propagation speed.
Queuing Delay [1] :
Queuing delay is the time a job waits in a queue until it can be executed. It depends on congestion. It is the time difference between when the packet arrived Destination and when the packet data was processed or executed. It may be caused by mainly three reasons i.e. originating switches, intermediate switches or call receiver servicing switches.
Processing Delay [1] :
Processing delay is the time it takes routers to process the packet header. Processing of packets helps in detecting bit-level errors that occur during transmission of a packet to the destination. Processing delays in high-speed routers are typically on the order of microseconds or less.
In simple words, it is just the time taken to process packets.

2. Does the average RTT vary with different packet sizes? What aspects of latency (transmit, propagation, and queueing delay) might impact this and why?

Answer: Yes, the average RTT increases with packet size. This is because queuing and transmission delay are dependent on the size of the packets and hence increase with increase in average RTT.

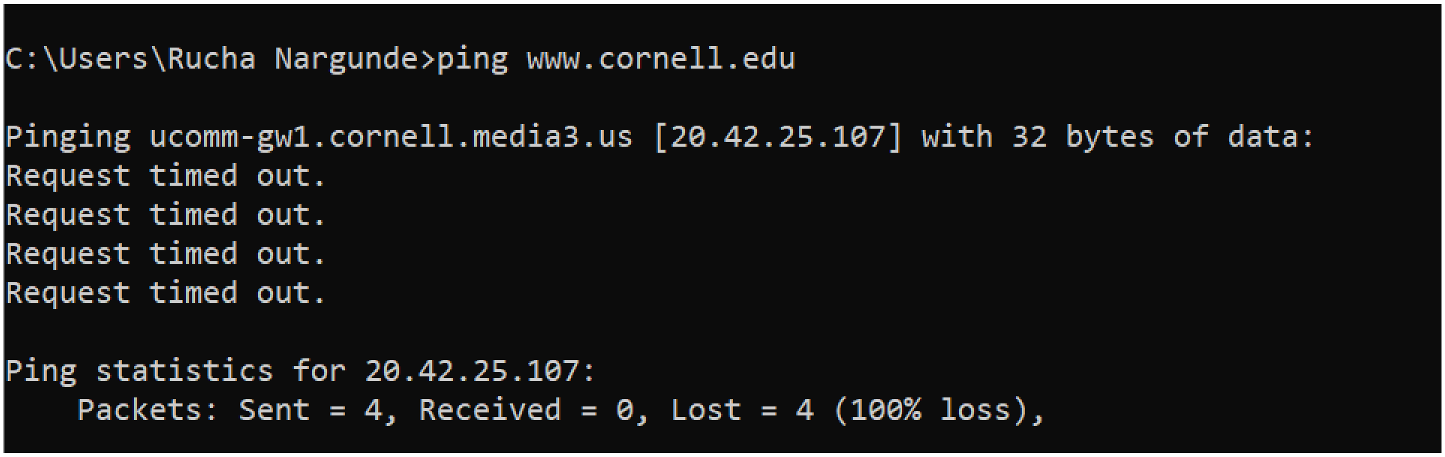
Exercise 1: Experiment with ping to find the round trip times to a variety of destinations. Write up any interesting observations, including in particular how the round trip time compares to the physical distance. Here are few places from who to get replies: www.uw.edu, www.cornell.edu, berkeley.edu, www.uchicago.edu, www.ox.ac.uk (England), www.u-tokyo.ac.jp (Japan).

Pinging www.uw.edu



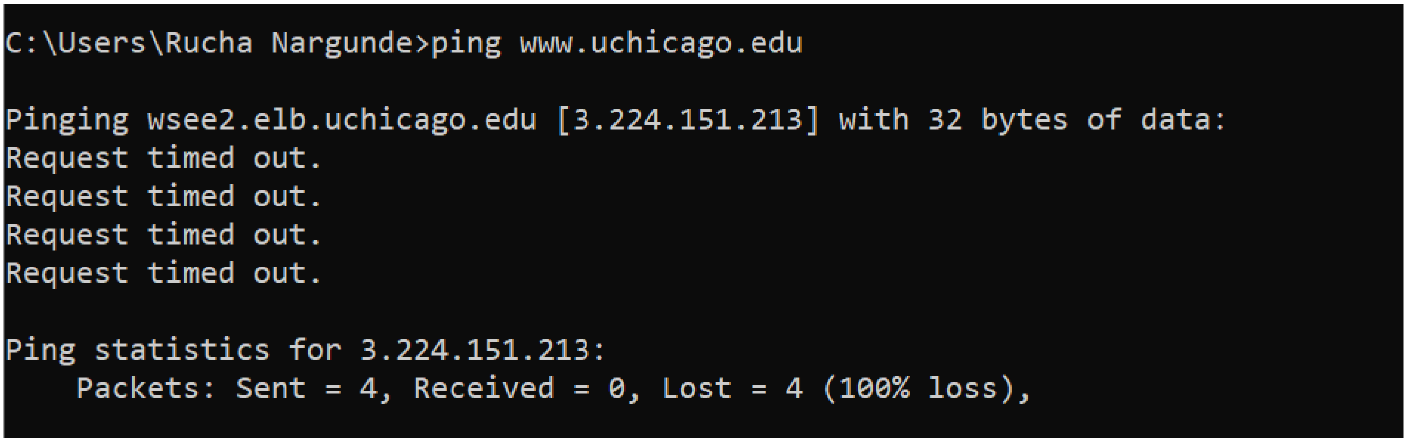
```
Microsoft Windows [Version 10.0.18362.1016]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Rucha Nargunde>ping www.uw.edu

Pinging www.washington.edu [128.95.155.134] with 32 bytes of data:
Reply from 128.95.155.134: bytes=32 time=321ms TTL=44
Reply from 128.95.155.134: bytes=32 time=252ms TTL=44
Reply from 128.95.155.134: bytes=32 time=252ms TTL=44
Reply from 128.95.155.134: bytes=32 time=250ms TTL=44

Ping statistics for 128.95.155.134:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 250ms, Maximum = 321ms, Average = 268ms
```

Pinging www.cornell.edu



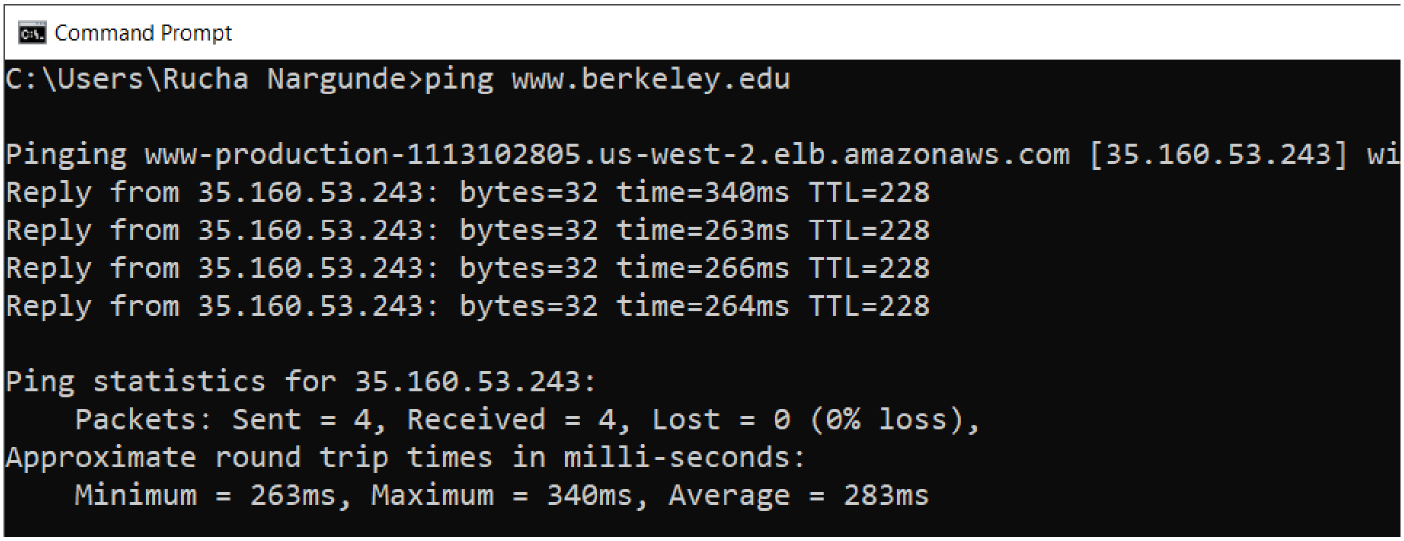
```
C:\Users\Rucha Nargunde>ping www.cornell.edu

Pinging ucomm-gw1.cornell.media3.us [20.42.25.107] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 20.42.25.107:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pinging www.uchicago.edu



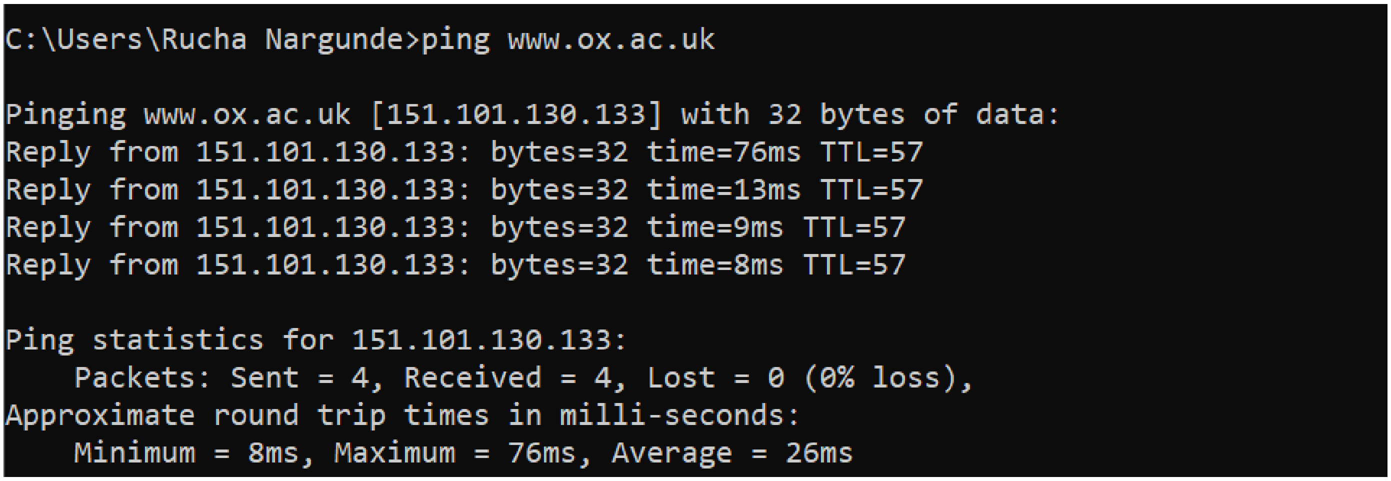
```
C:\Users\Rucha Nargunde>ping www.uchicago.edu

Pinging wsee2.elb.uchicago.edu [3.224.151.213] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 3.224.151.213:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pinging www.berkeley.edu



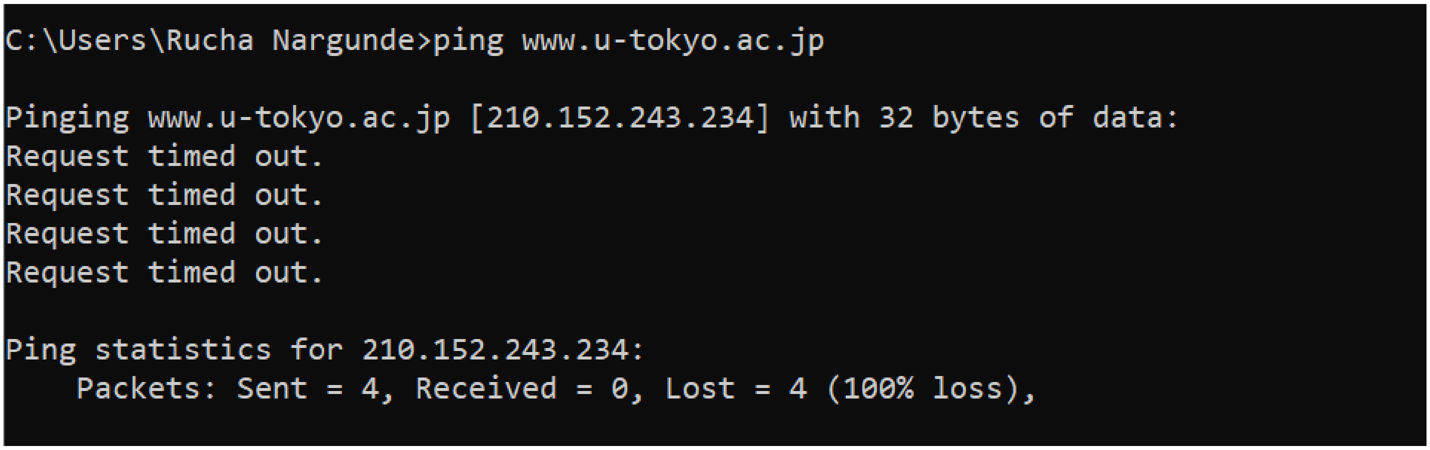
```
C:\Users\Rucha Nargunde>ping www.berkeley.edu

Pinging www-production-1113102805.us-west-2.elb.amazonaws.com [35.160.53.243] wi
Reply from 35.160.53.243: bytes=32 time=340ms TTL=228
Reply from 35.160.53.243: bytes=32 time=263ms TTL=228
Reply from 35.160.53.243: bytes=32 time=266ms TTL=228
Reply from 35.160.53.243: bytes=32 time=264ms TTL=228

Ping statistics for 35.160.53.243:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 263ms, Maximum = 340ms, Average = 283ms
```

Pinging www.ox.ac.uk



```
C:\Users\Rucha Nargunde>ping www.ox.ac.uk

Pinging www.ox.ac.uk [151.101.130.133] with 32 bytes of data:
Reply from 151.101.130.133: bytes=32 time=76ms TTL=57
Reply from 151.101.130.133: bytes=32 time=13ms TTL=57
Reply from 151.101.130.133: bytes=32 time=9ms TTL=57
Reply from 151.101.130.133: bytes=32 time=8ms TTL=57

Ping statistics for 151.101.130.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 76ms, Average = 26ms
```

Pinging www.u.tokyo.ac.jp

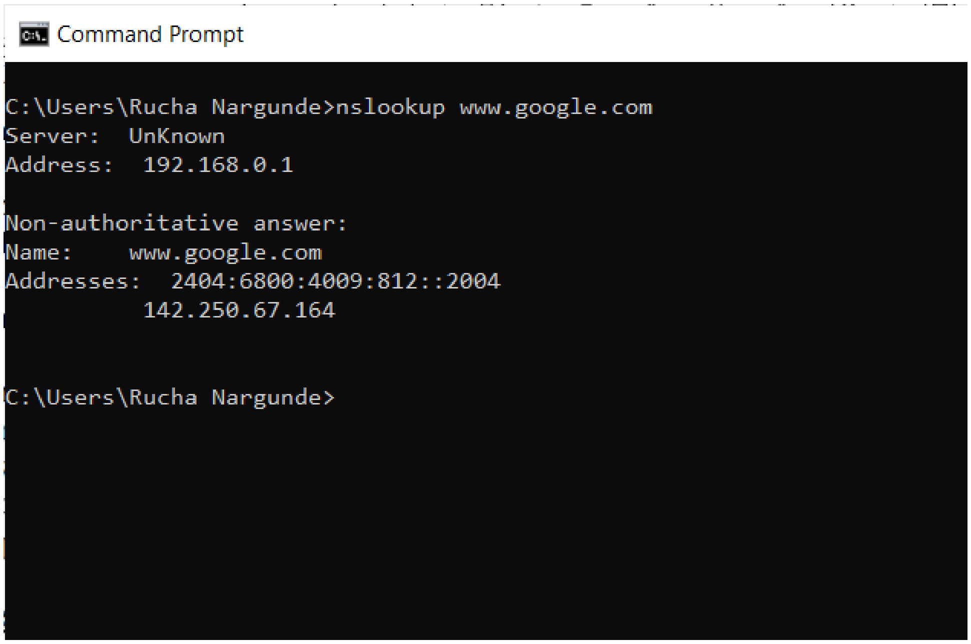


```
C:\Users\Rucha Nargunde>ping www.u-tokyo.ac.jp

Pinging www.u-tokyo.ac.jp [210.152.243.234] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 210.152.243.234:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

List of factors affecting the RTT [2]:

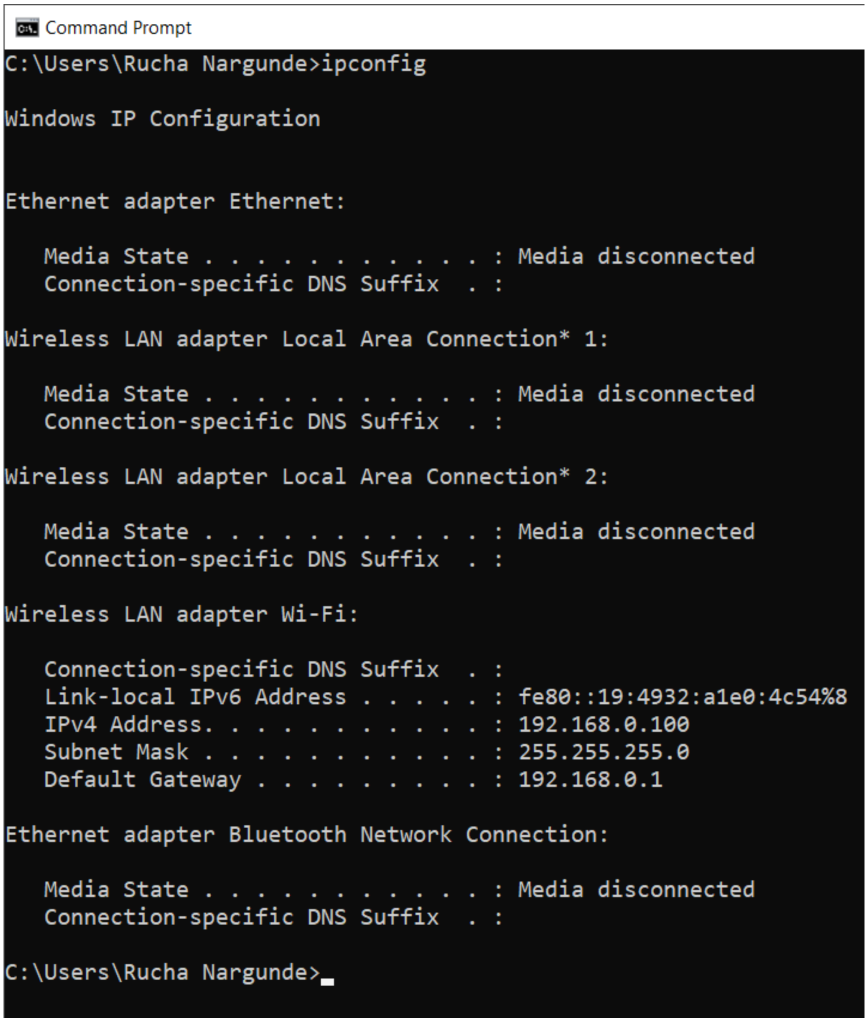
- **The nature of the transmission medium** - the way in which connections are made affects how fast the connection moves; connections made over optical fiber will behave differently than connections made over copper. Likewise, a connection made over a wireless frequency will behave differently than that of a satellite communication.
- **Local area network (LAN) traffic** - the amount of traffic on the local area network can bottleneck a connection before it ever reaches the larger Internet. For example, if many users are using streaming video service simultaneously, round-trip time may be inhibited even though the external network has excess capacity and is functioning normally.
- **Server response time** – the amount of time it takes a server to process and respond to a request is a potential bottleneck in network latency. When a server is overwhelmed with requests, such as during a DDoS attack, its ability to respond efficiently can be inhibited, resulting in increased RTT.
- **Node count and congestion –** depending on the path that a connection takes across the Internet, it may be routed or "hop" through a different number of intermediate nodes. Generally speaking, the greater the number of nodes a connection touches the slower it will be. A node may also experience network congestion from other network traffic, which will slow down the connection and increase RTT.
- **Physical distance** – although a connection optimized by a CDN can often reduce the number of hops required to reach a destination, there is no way of getting around the limitation imposed by the speed of light; the distance between a start and end point is a limiting factor in network connectivity that can only be reduced by moving content closer to the requesting users. To overcome this obstacle, a CDN will cache content closer to the requesting users, thereby reducing RTT.

nslookup — The command nslookup <host> will do a DNS query to find and report the IP address (or addresses) for a domain name or the domain name corresponding to an IP address. To do this, it contacts a "DNS server." Default DNS servers are part of a computer's network configuration. (For a static IP address in Linux, they are configured in the file /etc/network/interfaces that you encountered in the last lab.) You can specify a different DNS server to be used by nslokup by adding the server name or IP address to the command: nslookup <host> <server>



```
C:\Users\Rucha Nargunde>nslookup www.google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4009:812::2004
          142.250.67.164


C:\Users\Rucha Nargunde>
```

ifconfig — You used ifconfig in the previous lab. When used with no parameters, ifconfig reports some information about the computer's network interfaces. This usually includes lo which stands for localhost; it can be used for communication between programs running on the same computer. Linux often has an interface named eth0, which is the first ethernet card. The information is different on Mac OS and Linux, but includes the IP or "inet" address and ethernet or "hardware" address for an ethernet card. On Linux, you get the number of packets received (RX) and sent (TX), as well as the number of bytes transmitted and received. (A better place to monitor network bytes on our Linux computers is in the GUI program System Monitor, if it is installed!!!.)

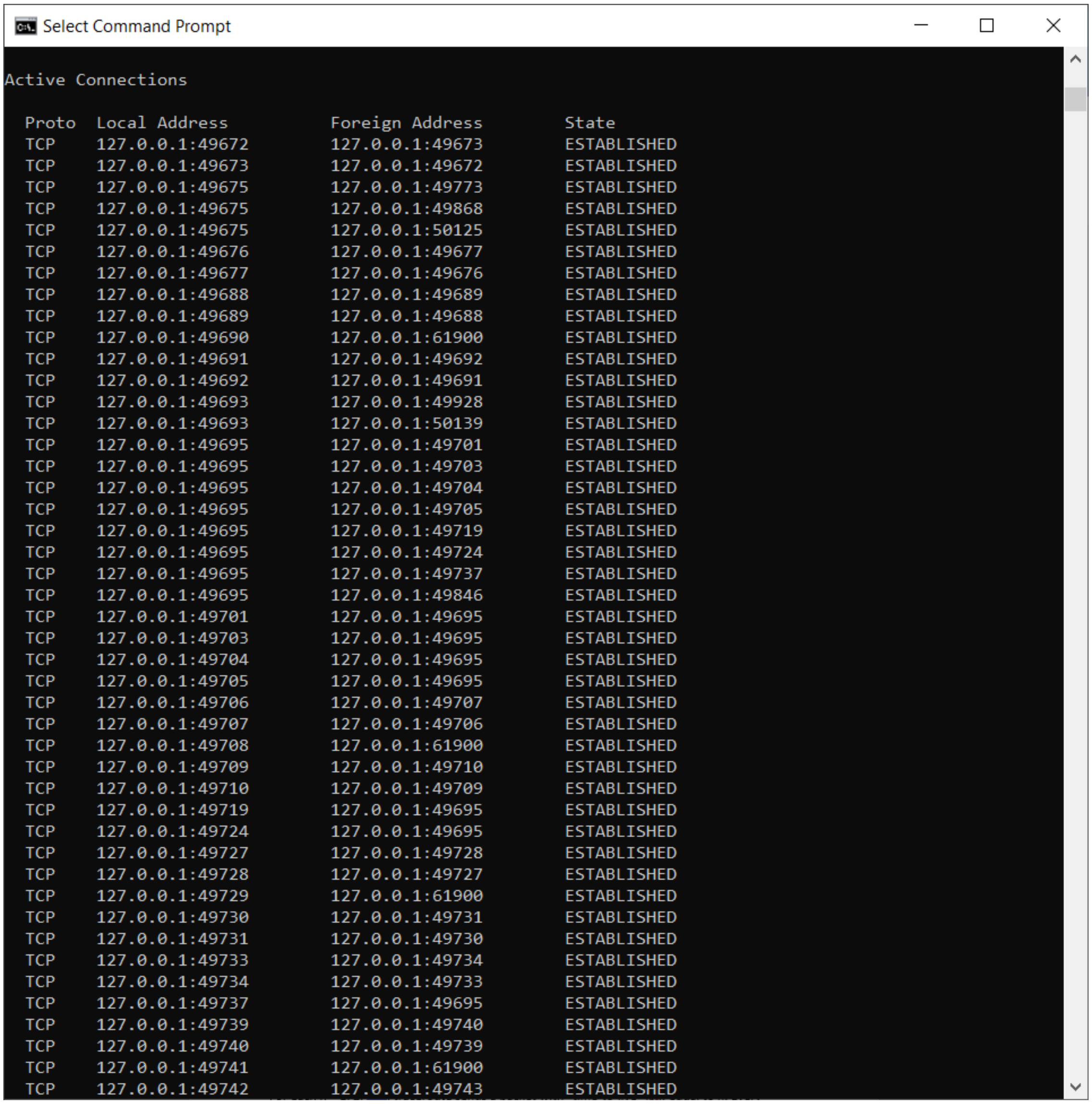


```
C:\Users\Rucha Nargunde>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::19:4932:a1e0:4c54%8
   IPv4 Address. . . . . . . . . . . : 192.168.0.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Rucha Nargunde>
```

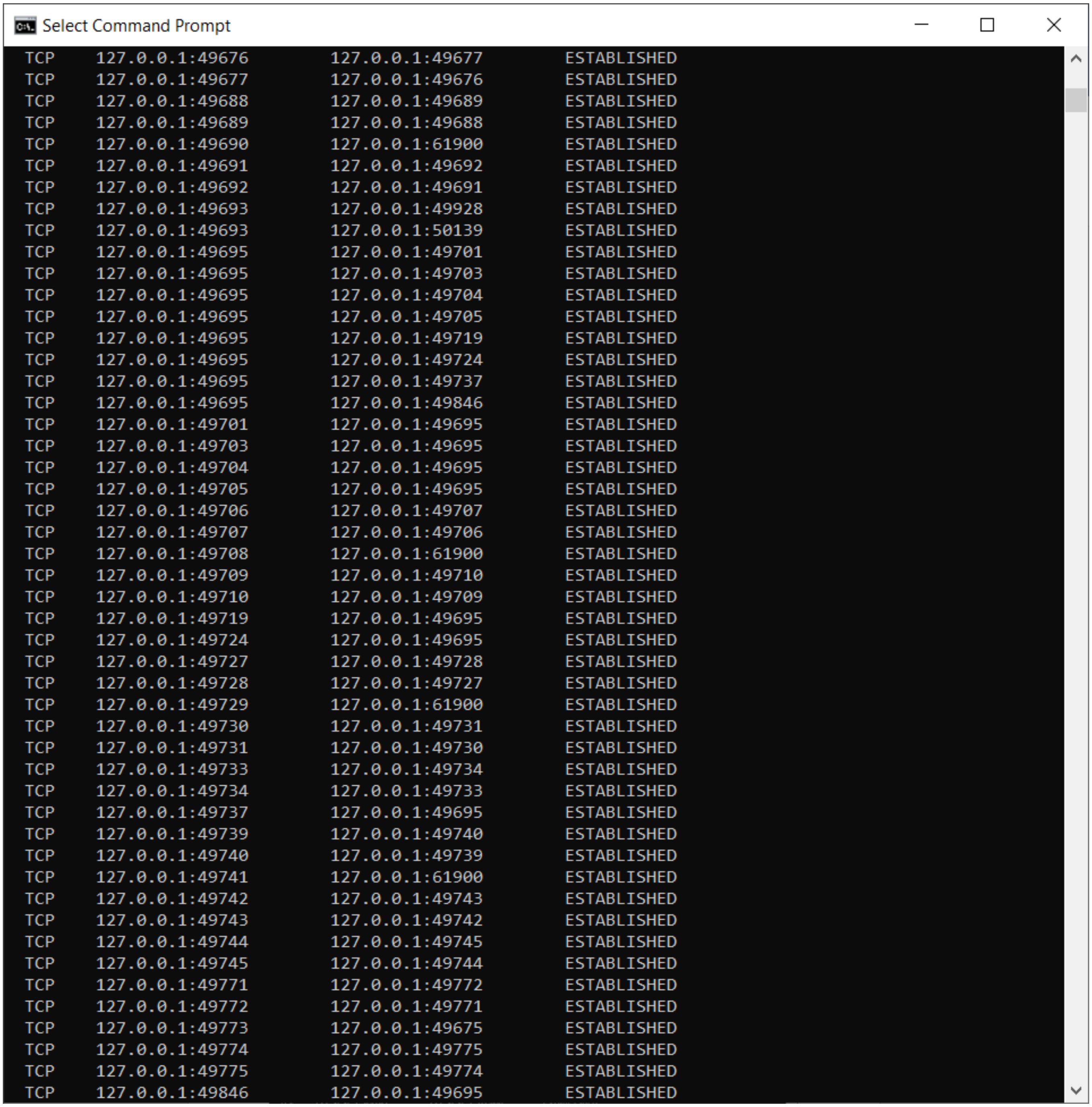
netstat — The netstat command gives information about network connections. I often use netstat -t -n which lists currently open TCP connections (that's the "-t" option) by IP address rather than domain name (that's the "-n" option). Add the option "-l" (lower case ell) to list listening sockets, that is sockets that have been opened by server programs to wait for connection requests from clients: netstat -t -n -l. (On Mac, use netstat -p tcp to list tcp connections, and add "-a" to include listening sockets in the list.)

Netstat [3] is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. **Netstat** provides information and statistics about protocols in use and current TCP/IP network connections. (The name derives from the words network and statistics.)

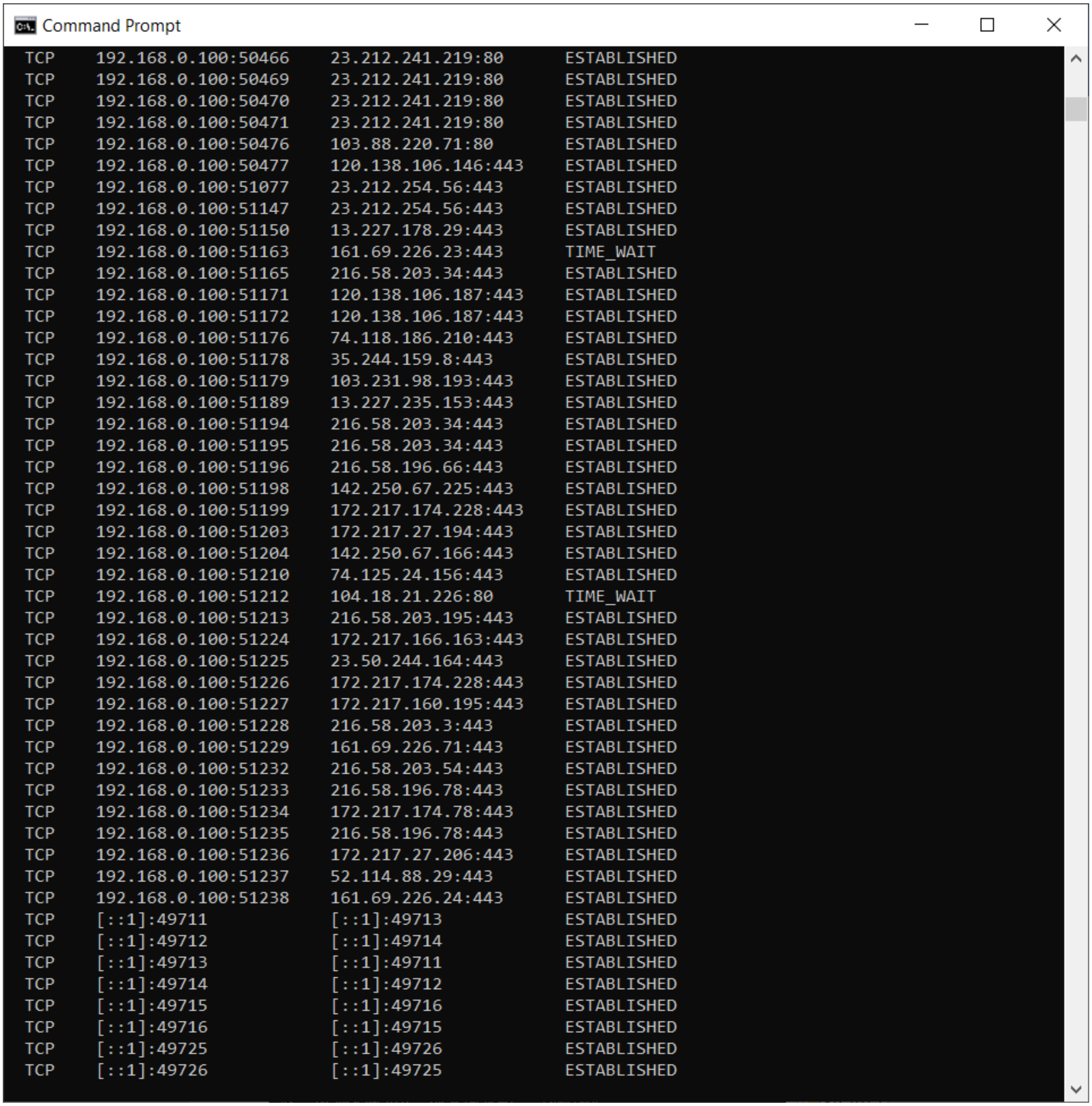
Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). [4]



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49672        127.0.0.1:49673        ESTABLISHED
  TCP    127.0.0.1:49673        127.0.0.1:49672        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:49773        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:49868        ESTABLISHED
  TCP    127.0.0.1:49675        127.0.0.1:50125        ESTABLISHED
  TCP    127.0.0.1:49676        127.0.0.1:49677        ESTABLISHED
  TCP    127.0.0.1:49677        127.0.0.1:49676        ESTABLISHED
  TCP    127.0.0.1:49688        127.0.0.1:49689        ESTABLISHED
  TCP    127.0.0.1:49689        127.0.0.1:49688        ESTABLISHED
  TCP    127.0.0.1:49690        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49691        127.0.0.1:49692        ESTABLISHED
  TCP    127.0.0.1:49692        127.0.0.1:49691        ESTABLISHED
  TCP    127.0.0.1:49693        127.0.0.1:49928        ESTABLISHED
  TCP    127.0.0.1:49693        127.0.0.1:50139        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49701        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49703        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49704        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49705        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49719        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49724        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49737        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49846        ESTABLISHED
  TCP    127.0.0.1:49701        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49703        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49704        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49705        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49706        127.0.0.1:49707        ESTABLISHED
  TCP    127.0.0.1:49707        127.0.0.1:49706        ESTABLISHED
  TCP    127.0.0.1:49708        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49709        127.0.0.1:49710        ESTABLISHED
  TCP    127.0.0.1:49710        127.0.0.1:49709        ESTABLISHED
  TCP    127.0.0.1:49719        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49724        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49727        127.0.0.1:49728        ESTABLISHED
  TCP    127.0.0.1:49728        127.0.0.1:49727        ESTABLISHED
  TCP    127.0.0.1:49729        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49730        127.0.0.1:49731        ESTABLISHED
  TCP    127.0.0.1:49731        127.0.0.1:49730        ESTABLISHED
  TCP    127.0.0.1:49733        127.0.0.1:49734        ESTABLISHED
  TCP    127.0.0.1:49734        127.0.0.1:49733        ESTABLISHED
  TCP    127.0.0.1:49737        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49739        127.0.0.1:49740        ESTABLISHED
  TCP    127.0.0.1:49740        127.0.0.1:49739        ESTABLISHED
  TCP    127.0.0.1:49741        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49742        127.0.0.1:49743        ESTABLISHED
```



```
  TCP    127.0.0.1:49676        127.0.0.1:49677        ESTABLISHED
  TCP    127.0.0.1:49677        127.0.0.1:49676        ESTABLISHED
  TCP    127.0.0.1:49688        127.0.0.1:49689        ESTABLISHED
  TCP    127.0.0.1:49689        127.0.0.1:49688        ESTABLISHED
  TCP    127.0.0.1:49690        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49691        127.0.0.1:49692        ESTABLISHED
  TCP    127.0.0.1:49692        127.0.0.1:49691        ESTABLISHED
  TCP    127.0.0.1:49693        127.0.0.1:49928        ESTABLISHED
  TCP    127.0.0.1:49693        127.0.0.1:50139        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49701        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49703        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49704        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49705        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49719        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49724        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49737        ESTABLISHED
  TCP    127.0.0.1:49695        127.0.0.1:49846        ESTABLISHED
  TCP    127.0.0.1:49701        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49703        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49704        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49705        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49706        127.0.0.1:49707        ESTABLISHED
  TCP    127.0.0.1:49707        127.0.0.1:49706        ESTABLISHED
  TCP    127.0.0.1:49708        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49709        127.0.0.1:49710        ESTABLISHED
  TCP    127.0.0.1:49710        127.0.0.1:49709        ESTABLISHED
  TCP    127.0.0.1:49719        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49724        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49727        127.0.0.1:49728        ESTABLISHED
  TCP    127.0.0.1:49728        127.0.0.1:49727        ESTABLISHED
  TCP    127.0.0.1:49729        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49730        127.0.0.1:49731        ESTABLISHED
  TCP    127.0.0.1:49731        127.0.0.1:49730        ESTABLISHED
  TCP    127.0.0.1:49733        127.0.0.1:49734        ESTABLISHED
  TCP    127.0.0.1:49734        127.0.0.1:49733        ESTABLISHED
  TCP    127.0.0.1:49737        127.0.0.1:49695        ESTABLISHED
  TCP    127.0.0.1:49739        127.0.0.1:49740        ESTABLISHED
  TCP    127.0.0.1:49740        127.0.0.1:49739        ESTABLISHED
  TCP    127.0.0.1:49741        127.0.0.1:61900        ESTABLISHED
  TCP    127.0.0.1:49742        127.0.0.1:49743        ESTABLISHED
  TCP    127.0.0.1:49743        127.0.0.1:49742        ESTABLISHED
  TCP    127.0.0.1:49744        127.0.0.1:49745        ESTABLISHED
  TCP    127.0.0.1:49745        127.0.0.1:49744        ESTABLISHED
  TCP    127.0.0.1:49771        127.0.0.1:49772        ESTABLISHED
  TCP    127.0.0.1:49772        127.0.0.1:49771        ESTABLISHED
  TCP    127.0.0.1:49773        127.0.0.1:49675        ESTABLISHED
  TCP    127.0.0.1:49774        127.0.0.1:49775        ESTABLISHED
  TCP    127.0.0.1:49775        127.0.0.1:49774        ESTABLISHED
  TCP    127.0.0.1:49846        127.0.0.1:49695        ESTABLISHED
```



```
  TCP    192.168.0.100:50466    23.212.241.219:80      ESTABLISHED
  TCP    192.168.0.100:50469    23.212.241.219:80      ESTABLISHED
  TCP    192.168.0.100:50470    23.212.241.219:80      ESTABLISHED
  TCP    192.168.0.100:50471    23.212.241.219:80      ESTABLISHED
  TCP    192.168.0.100:50476    103.88.220.71:80       ESTABLISHED
  TCP    192.168.0.100:50477    120.138.106.146:443    ESTABLISHED
  TCP    192.168.0.100:51077    23.212.254.56:443      ESTABLISHED
  TCP    192.168.0.100:51147    23.212.254.56:443      ESTABLISHED
  TCP    192.168.0.100:51150    13.227.178.29:443      ESTABLISHED
  TCP    192.168.0.100:51163    161.69.226.23:443      TIME_WAIT
  TCP    192.168.0.100:51165    216.58.203.34:443      ESTABLISHED
  TCP    192.168.0.100:51171    120.138.106.187:443    ESTABLISHED
  TCP    192.168.0.100:51172    120.138.106.187:443    ESTABLISHED
  TCP    192.168.0.100:51176    74.118.186.210:443     ESTABLISHED
  TCP    192.168.0.100:51178    35.244.159.8:443       ESTABLISHED
  TCP    192.168.0.100:51179    103.231.98.193:443     ESTABLISHED
  TCP    192.168.0.100:51189    13.227.235.153:443     ESTABLISHED
  TCP    192.168.0.100:51194    216.58.203.34:443      ESTABLISHED
  TCP    192.168.0.100:51195    216.58.203.34:443      ESTABLISHED
  TCP    192.168.0.100:51196    216.58.196.66:443      ESTABLISHED
  TCP    192.168.0.100:51198    142.250.67.225:443     ESTABLISHED
  TCP    192.168.0.100:51199    172.217.174.228:443    ESTABLISHED
  TCP    192.168.0.100:51203    172.217.27.194:443     ESTABLISHED
  TCP    192.168.0.100:51204    142.250.67.166:443     ESTABLISHED
  TCP    192.168.0.100:51210    74.125.24.156:443      ESTABLISHED
  TCP    192.168.0.100:51212    104.18.21.226:80       TIME_WAIT
  TCP    192.168.0.100:51213    216.58.203.195:443     ESTABLISHED
  TCP    192.168.0.100:51224    172.217.166.163:443    ESTABLISHED
  TCP    192.168.0.100:51225    23.50.244.164:443      ESTABLISHED
  TCP    192.168.0.100:51226    172.217.174.228:443    ESTABLISHED
  TCP    192.168.0.100:51227    172.217.160.195:443    ESTABLISHED
  TCP    192.168.0.100:51228    216.58.203.3:443       ESTABLISHED
  TCP    192.168.0.100:51229    161.69.226.71:443      ESTABLISHED
  TCP    192.168.0.100:51232    216.58.203.54:443      ESTABLISHED
  TCP    192.168.0.100:51233    216.58.196.78:443      ESTABLISHED
  TCP    192.168.0.100:51234    172.217.174.78:443     ESTABLISHED
  TCP    192.168.0.100:51235    216.58.196.78:443      ESTABLISHED
  TCP    192.168.0.100:51236    172.217.27.206:443     ESTABLISHED
  TCP    192.168.0.100:51237    52.114.88.29:443       ESTABLISHED
  TCP    192.168.0.100:51238    161.69.226.24:443      ESTABLISHED
  TCP    [::1]:49711            [::1]:49713            ESTABLISHED
  TCP    [::1]:49712            [::1]:49714            ESTABLISHED
  TCP    [::1]:49713            [::1]:49711            ESTABLISHED
  TCP    [::1]:49714            [::1]:49712            ESTABLISHED
  TCP    [::1]:49715            [::1]:49716            ESTABLISHED
  TCP    [::1]:49716            [::1]:49715            ESTABLISHED
  TCP    [::1]:49725            [::1]:49726            ESTABLISHED
  TCP    [::1]:49726            [::1]:49725            ESTABLISHED
```

telnet — Telnet is an old program for remote login. It's not used so much for that any more, since it has no security features. But basically, all it does is open a connection to a server and allow server and client to send lines of plain text to each other. It can be used to check that it's possible to connect to a server and, if the server communicates in plain text, even to interact with the server by hand. Since the Web uses a plain text protocol, you can use telnet to connect to a web client and play the part of the web browser. I will suggest that you to do this with your own web server when you write it, but you might want to try it now. When you use telnet in this way, you need to specify both the host and the port number to which you want to connect: telent <host> <port>. For example, to connect to the web server on www.spit.ac.in: telnet spit.ac.in 80

traceroute — Traceroute is discussed in man utility. The command traceroute <host> will show routers encountered by packets on their way from your computer to a specified <host>. For each n = 1, 2, 3,..., traceroute sends a packet with "time-to-live" (ttl) equal to n. Every time a router forwards a packet, it decreases the ttl of the packet by one. If the ttl drops to zero, the router discards the packet and sends an error message back to the sender of the packet. (Again, as with ping, the packets might be blocked or might not even be sent, so that the error messages will never be received.) The sender gets the identity of the router from the source of the error message. Traceroute will send packets until n reaches some set upper bound or until a packet actually gets through to the destination. It actually does this three times for each n. In this way, it identifies routers that are one step, two steps, three steps, ... away from the source computer. A packet for which no response is received is indicated in the output as a *.

Traceroute is installed on the computers. If was not installed in your virtual server last week, but you can install it with the command sudo apt-get install traceroute

The path taken through a network, can be measured using traceroute. The syntax for the command in Linux is:

```
traceroute <hostname>
```

The syntax in Windows is:

```
tracert <hostname>
```

You can specify either a hostname (e.g., cs.iitb.ac.in) or an IP address (e.g., 128.105.2.6).

Traceroute [5] is a command line utility that measures the speed and route data takes to a destination server.It works by sending several test packets of data to a specified destination address, and records each intermediate router or link passed by the data on it's journey.

Output of traceroute explanation [6]:

```
10    81 ms    74 ms    74 ms  205.134.225.38
```

Let’s break this particular hop down into its parts.

Hop #	RTT 1	RTT 2	RTT 3	Name/IP Address
10	81 ms	74 ms	74 ms	205.134.225.38

- Hop Number – This is the first column and is simply the number of the hop along the route. In this case, it is the tenth hop.

- RTT Columns – The next three columns display the round trip time (RTT) for your packet to reach that point and return to your computer. This is listed in milliseconds. There are three columns because the traceroute sends three separate signal packets. This is to display consistency, or a lack thereof, in the route.

- Domain/IP column – The last column has the IP address of the router. If it is available, the domain name will also be listed.

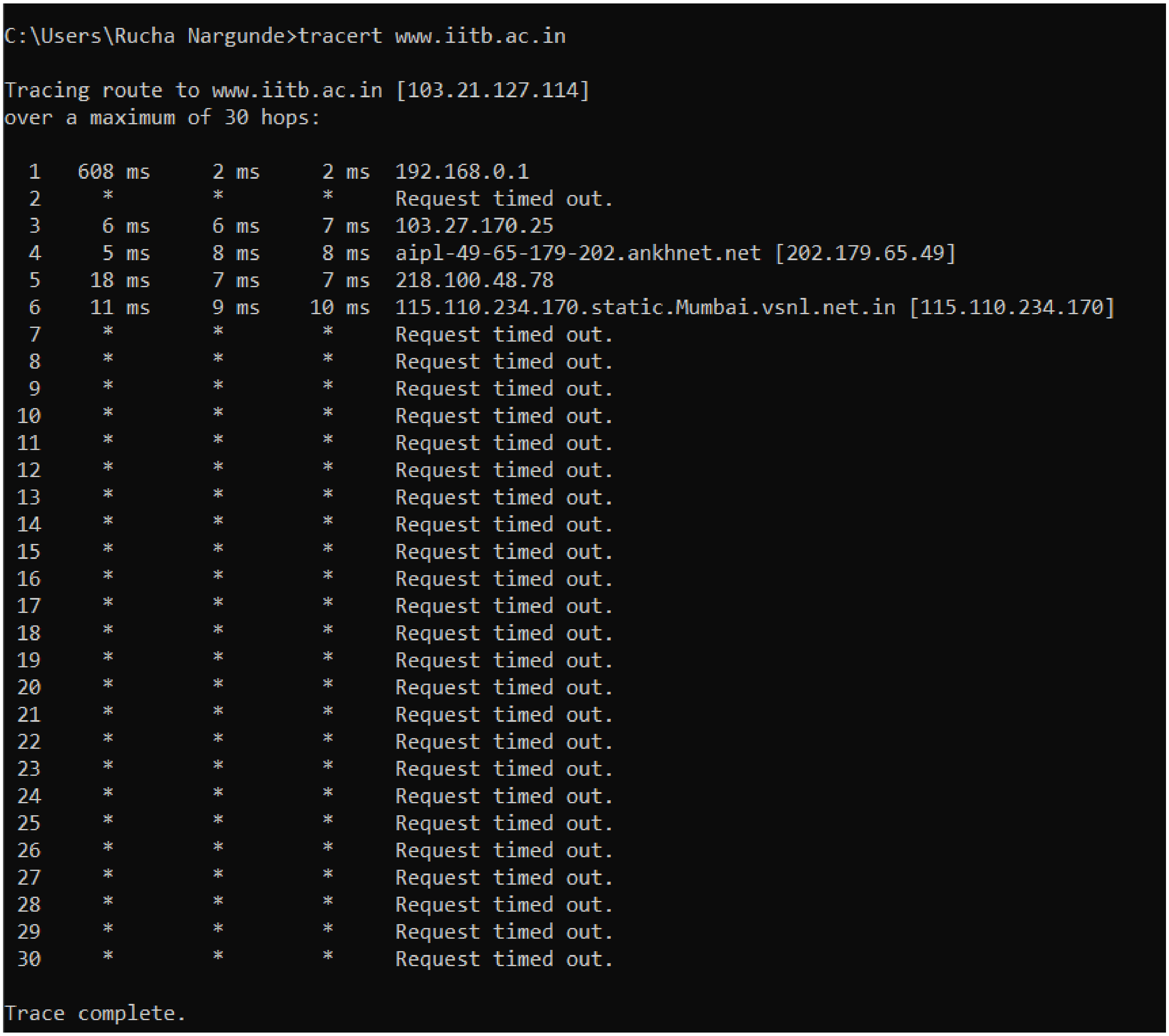
1.2.1 EXPERIMENTS WITH TRACEROUTE

From **your machine** traceroute to the following hosts:

1. ee.iitb.ac.in
2. mscs.mu.edu
3. www.cs.grinnell.edu
4. csail.mit.edu
5. cs.stanford.edu
6. cs.manchester.ac.uk

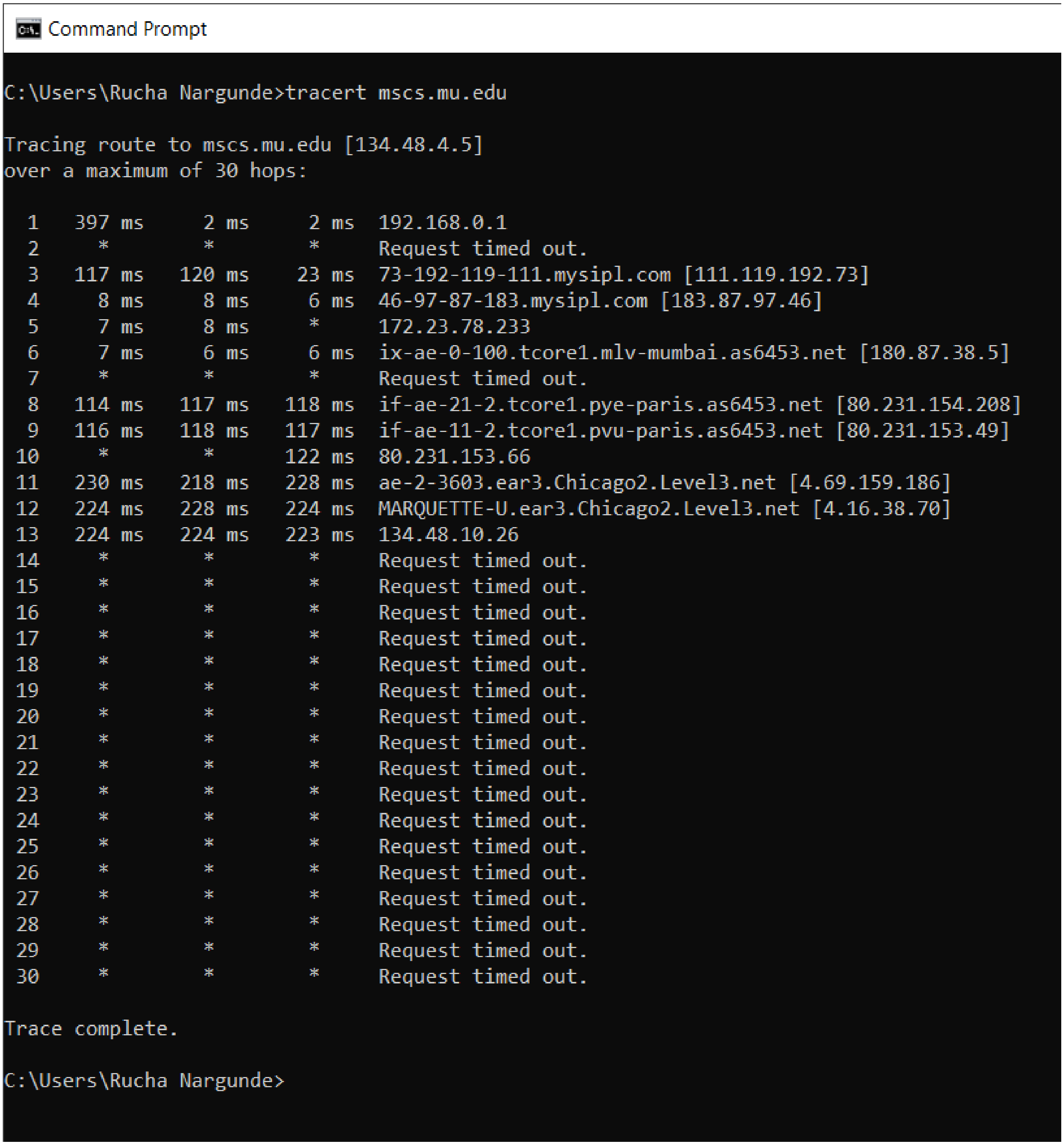
Store the output of each traceroute command in a separate file named traceroute_HOSTNAME.log, replacing HOSTNAME with the hostname for end-host you pinged
(e.g., traceroute_ee.iitb.ac.in.log).

Tracing route to www.iitb.ac.in



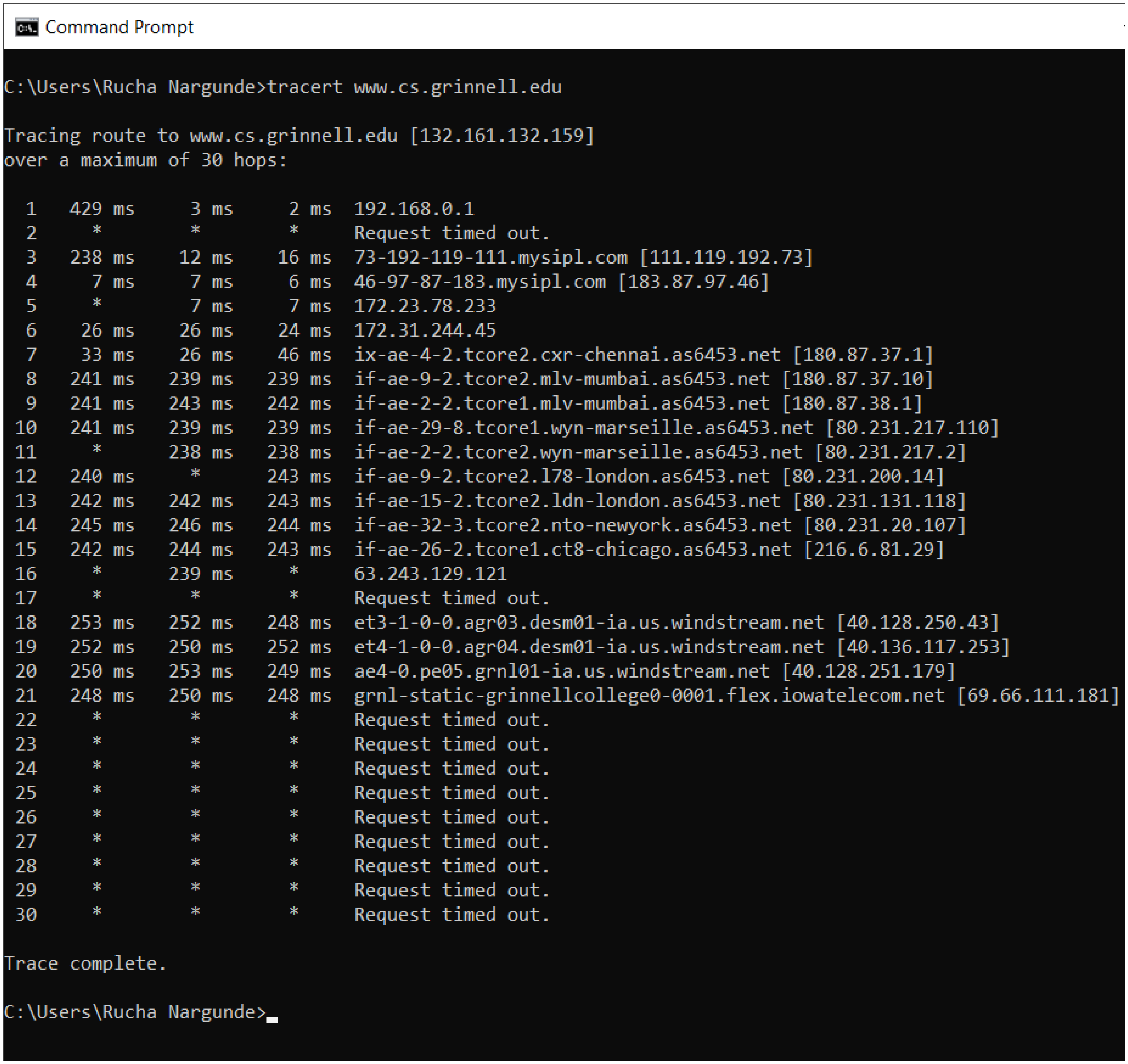
```
C:\Users\Rucha Nargunde>tracert www.iitb.ac.in

Tracing route to www.iitb.ac.in [103.21.127.114]
over a maximum of 30 hops:

  1   608 ms     2 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     6 ms     6 ms     7 ms  103.27.170.25
  4     5 ms     8 ms     8 ms  aipl-49-65-179-202.ankhnet.net [202.179.65.49]
  5    18 ms     7 ms     7 ms  218.100.48.78
  6    11 ms     9 ms    10 ms  115.110.234.170.static.Mumbai.vsnl.net.in [115.110.234.170]
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12     *        *        *     Request timed out.
 13     *        *        *     Request timed out.
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

Tracing route to mscs.mu.edu



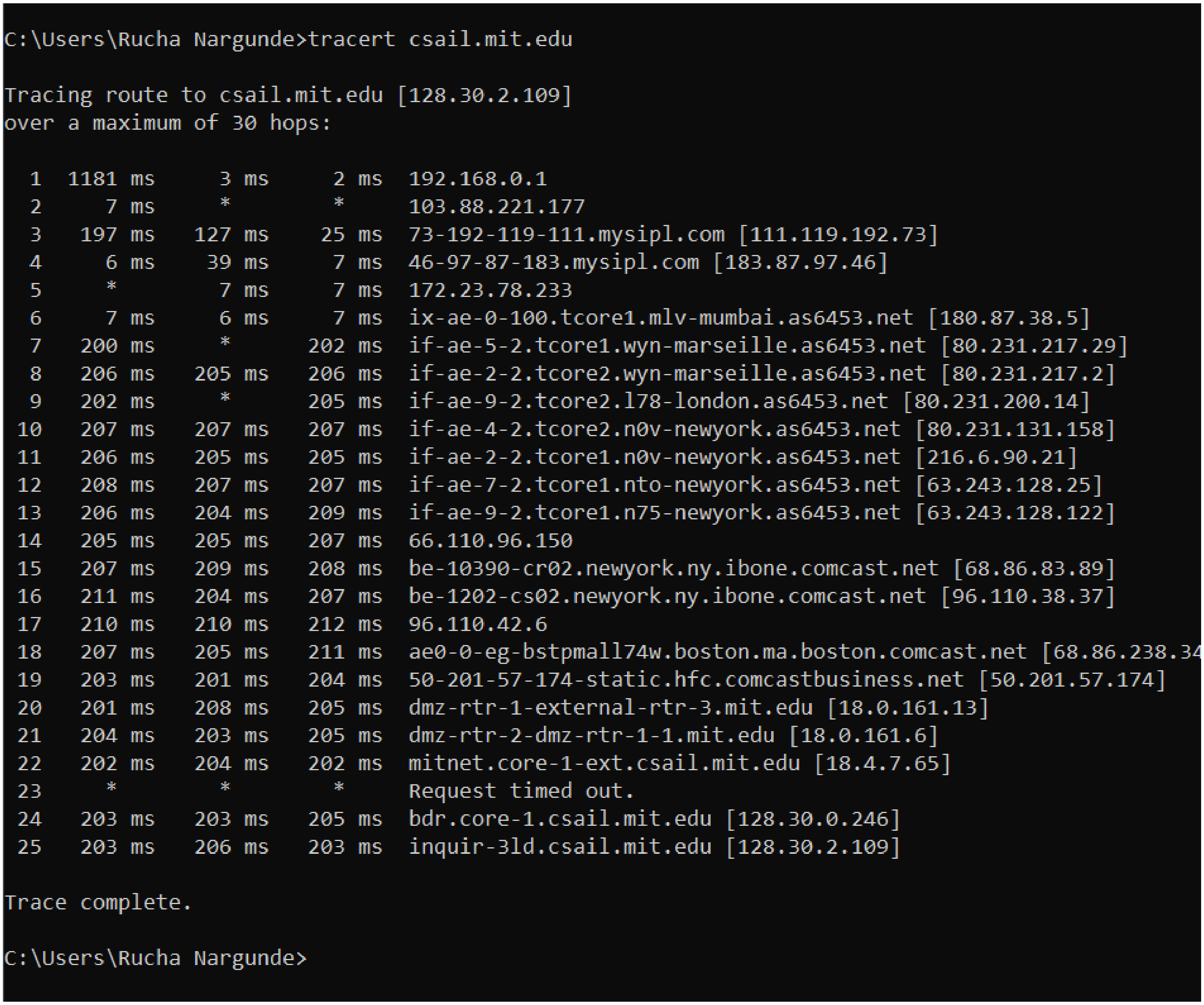
```
C:\Users\Rucha Nargunde>tracert mscs.mu.edu

Tracing route to mscs.mu.edu [134.48.4.5]
over a maximum of 30 hops:

  1   397 ms     2 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3   117 ms   120 ms    23 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4     8 ms     8 ms     6 ms  46-97-87-183.mysipl.com [183.87.97.46]
  5     7 ms     8 ms     *     172.23.78.233
  6     7 ms     6 ms     6 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7     *        *        *     Request timed out.
  8   114 ms   117 ms   118 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  9   116 ms   118 ms   117 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *      122 ms  80.231.153.66
 11   230 ms   218 ms   228 ms  ae-2-3603.ear3.Chicago2.Level3.net [4.69.159.186]
 12   224 ms   228 ms   224 ms  MARQUETTE-U.ear3.Chicago2.Level3.net [4.16.38.70]
 13   224 ms   224 ms   223 ms  134.48.10.26
 14     *        *        *     Request timed out.
 15     *        *        *     Request timed out.
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\Rucha Nargunde>
```

Tracing route to www.cs.grinnell.edu



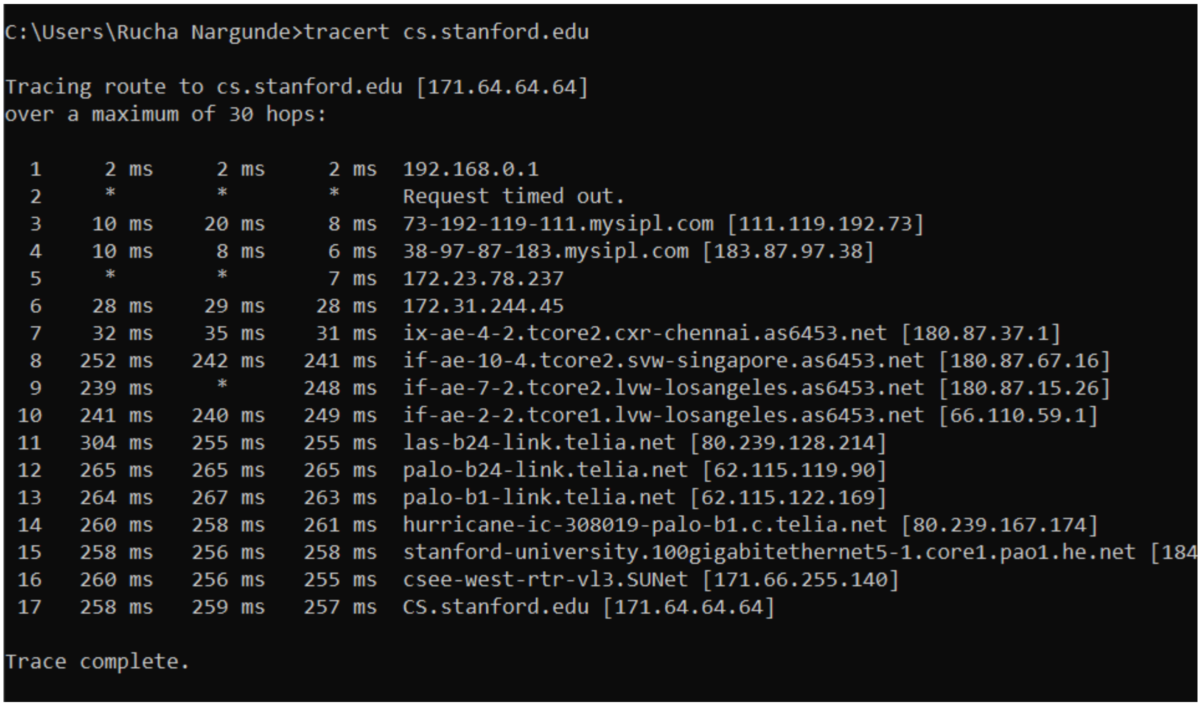
```
C:\Users\Rucha Nargunde>tracert www.cs.grinnell.edu

Tracing route to www.cs.grinnell.edu [132.161.132.159]
over a maximum of 30 hops:

  1   429 ms     3 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3   238 ms    12 ms    16 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4     7 ms     7 ms     6 ms  46-97-87-183.mysipl.com [183.87.97.46]
  5     *        7 ms     7 ms  172.23.78.233
  6    26 ms    26 ms    24 ms  172.31.244.45
  7    33 ms    26 ms    46 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
  8   241 ms   239 ms   239 ms  if-ae-9-2.tcore2.mlv-mumbai.as6453.net [180.87.37.10]
  9   241 ms   243 ms   242 ms  if-ae-2-2.tcore1.mlv-mumbai.as6453.net [180.87.38.1]
 10   241 ms   239 ms   239 ms  if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
 11     *      238 ms   238 ms  if-ae-2-2.tcore2.wyn-marseille.as6453.net [80.231.217.2]
 12   240 ms     *      243 ms  if-ae-9-2.tcore2.l78-london.as6453.net [80.231.200.14]
 13   242 ms   242 ms   243 ms  if-ae-15-2.tcore2.ldn-london.as6453.net [80.231.131.118]
 14   245 ms   246 ms   244 ms  if-ae-32-3.tcore2.nto-newyork.as6453.net [80.231.20.107]
 15   242 ms   244 ms   243 ms  if-ae-26-2.tcore1.ct8-chicago.as6453.net [216.6.81.29]
 16     *      239 ms     *     63.243.129.121
 17     *        *        *     Request timed out.
 18   253 ms   252 ms   248 ms  et3-1-0-0.agr03.desm01-ia.us.windstream.net [40.128.250.43]
 19   252 ms   250 ms   252 ms  et4-1-0-0.agr04.desm01-ia.us.windstream.net [40.136.117.253]
 20   250 ms   253 ms   249 ms  ae4-0.pe05.grnl01-ia.us.windstream.net [40.128.251.179]
 21   248 ms   250 ms   248 ms  grnl-static-grinnellcollege0-0001.flex.iowatelecom.net [69.66.111.181]
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.

C:\Users\Rucha Nargunde>
```

Tracing route to csail.mit.edu



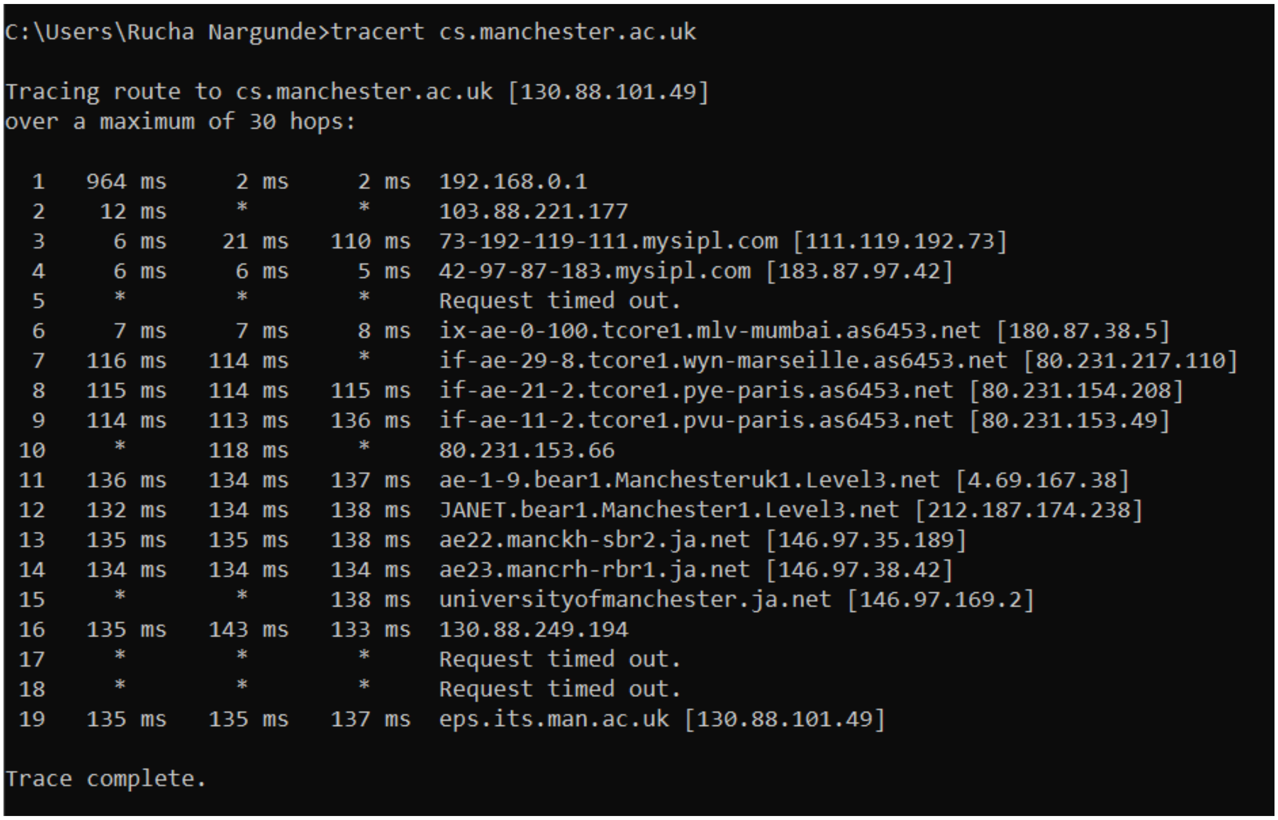
```
C:\Users\Rucha Nargunde>tracert csail.mit.edu

Tracing route to csail.mit.edu [128.30.2.109]
over a maximum of 30 hops:

  1  1181 ms     3 ms     2 ms  192.168.0.1
  2     7 ms     *        *     103.88.221.177
  3   197 ms   127 ms    25 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4     6 ms    39 ms     7 ms  46-97-87-183.mysipl.com [183.87.97.46]
  5     *        7 ms     7 ms  172.23.78.233
  6     7 ms     6 ms     7 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7   200 ms     *      202 ms  if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
  8   206 ms   205 ms   206 ms  if-ae-2-2.tcore2.wyn-marseille.as6453.net [80.231.217.2]
  9   202 ms     *      205 ms  if-ae-9-2.tcore2.l78-london.as6453.net [80.231.200.14]
 10   207 ms   207 ms   207 ms  if-ae-4-2.tcore2.n0v-newyork.as6453.net [80.231.131.158]
 11   206 ms   205 ms   205 ms  if-ae-2-2.tcore1.n0v-newyork.as6453.net [216.6.90.21]
 12   208 ms   207 ms   207 ms  if-ae-7-2.tcore1.nto-newyork.as6453.net [63.243.128.25]
 13   206 ms   204 ms   209 ms  if-ae-9-2.tcore1.n75-newyork.as6453.net [63.243.128.122]
 14   205 ms   205 ms   207 ms  66.110.96.150
 15   207 ms   209 ms   208 ms  be-10390-cr02.newyork.ny.ibone.comcast.net [68.86.83.89]
 16   211 ms   204 ms   207 ms  be-1202-cs02.newyork.ny.ibone.comcast.net [96.110.38.37]
 17   210 ms   210 ms   212 ms  96.110.42.6
 18   207 ms   205 ms   211 ms  ae0-0-eg-bstpmall74w.boston.ma.boston.comcast.net [68.86.238.34
 19   203 ms   201 ms   204 ms  50-201-57-174-static.hfc.comcastbusiness.net [50.201.57.174]
 20   201 ms   208 ms   205 ms  dmz-rtr-1-external-rtr-3.mit.edu [18.0.161.13]
 21   204 ms   203 ms   205 ms  dmz-rtr-2-dmz-rtr-1-1.mit.edu [18.0.161.6]
 22   202 ms   204 ms   202 ms  mitnet.core-1-ext.csail.mit.edu [18.4.7.65]
 23     *        *        *     Request timed out.
 24   203 ms   203 ms   205 ms  bdr.core-1.csail.mit.edu [128.30.0.246]
 25   203 ms   206 ms   203 ms  inquir-3ld.csail.mit.edu [128.30.2.109]

Trace complete.

C:\Users\Rucha Nargunde>
```

Tracing route to cs.stanford.edu



```
C:\Users\Rucha Nargunde>tracert cs.stanford.edu

Tracing route to cs.stanford.edu [171.64.64.64]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3    10 ms    20 ms     8 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4    10 ms     8 ms     6 ms  38-97-87-183.mysipl.com [183.87.97.38]
  5     *        *        7 ms  172.23.78.237
  6    28 ms    29 ms    28 ms  172.31.244.45
  7    32 ms    35 ms    31 ms  ix-ae-4-2.tcore2.cxr-chennai.as6453.net [180.87.37.1]
  8   252 ms   242 ms   241 ms  if-ae-10-4.tcore2.svw-singapore.as6453.net [180.87.67.16]
  9   239 ms     *      248 ms  if-ae-7-2.tcore2.lvw-losangeles.as6453.net [180.87.15.26]
 10   241 ms   240 ms   249 ms  if-ae-2-2.tcore1.lvw-losangeles.as6453.net [66.110.59.1]
 11   304 ms   255 ms   255 ms  las-b24-link.telia.net [80.239.128.214]
 12   265 ms   265 ms   265 ms  palo-b24-link.telia.net [62.115.119.90]
 13   264 ms   267 ms   263 ms  palo-b1-link.telia.net [62.115.122.169]
 14   260 ms   258 ms   261 ms  hurricane-ic-308019-palo-b1.c.telia.net [80.239.167.174]
 15   258 ms   256 ms   258 ms  stanford-university.100gigabitethernet5-1.core1.pao1.he.net [184
 16   260 ms   256 ms   255 ms  csee-west-rtr-vl3.SUNet [171.66.255.140]
 17   258 ms   259 ms   257 ms  CS.stanford.edu [171.64.64.64]

Trace complete.
```

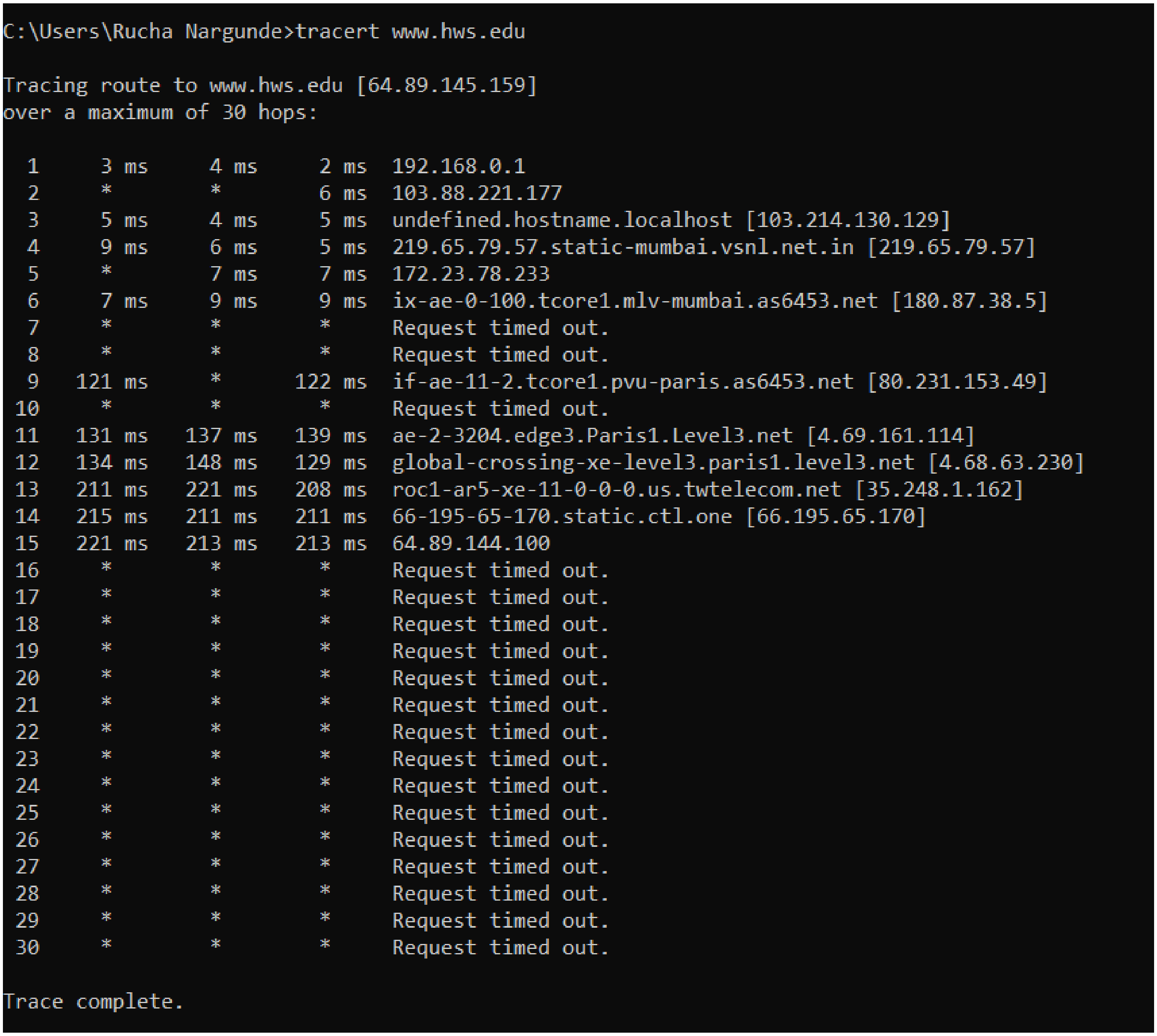
Tracing route to cs.manchester.ac.uk



```
C:\Users\Rucha Nargunde>tracert cs.manchester.ac.uk

Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1   964 ms     2 ms     2 ms  192.168.0.1
  2    12 ms     *        *     103.88.221.177
  3     6 ms    21 ms   110 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4     6 ms     6 ms     5 ms  42-97-87-183.mysipl.com [183.87.97.42]
  5     *        *        *     Request timed out.
  6     7 ms     7 ms     8 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7   116 ms   114 ms     *     if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
  8   115 ms   114 ms   115 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  9   114 ms   113 ms   136 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *      118 ms     *     80.231.153.66
 11   136 ms   134 ms   137 ms  ae-1-9.bear1.Manchesteruk1.Level3.net [4.69.167.38]
 12   132 ms   134 ms   138 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 13   135 ms   135 ms   138 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 14   134 ms   134 ms   134 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 15     *        *      138 ms  universityofmanchester.ja.net [146.97.169.2]
 16   135 ms   143 ms   133 ms  130.88.249.194
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19   135 ms   135 ms   137 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```

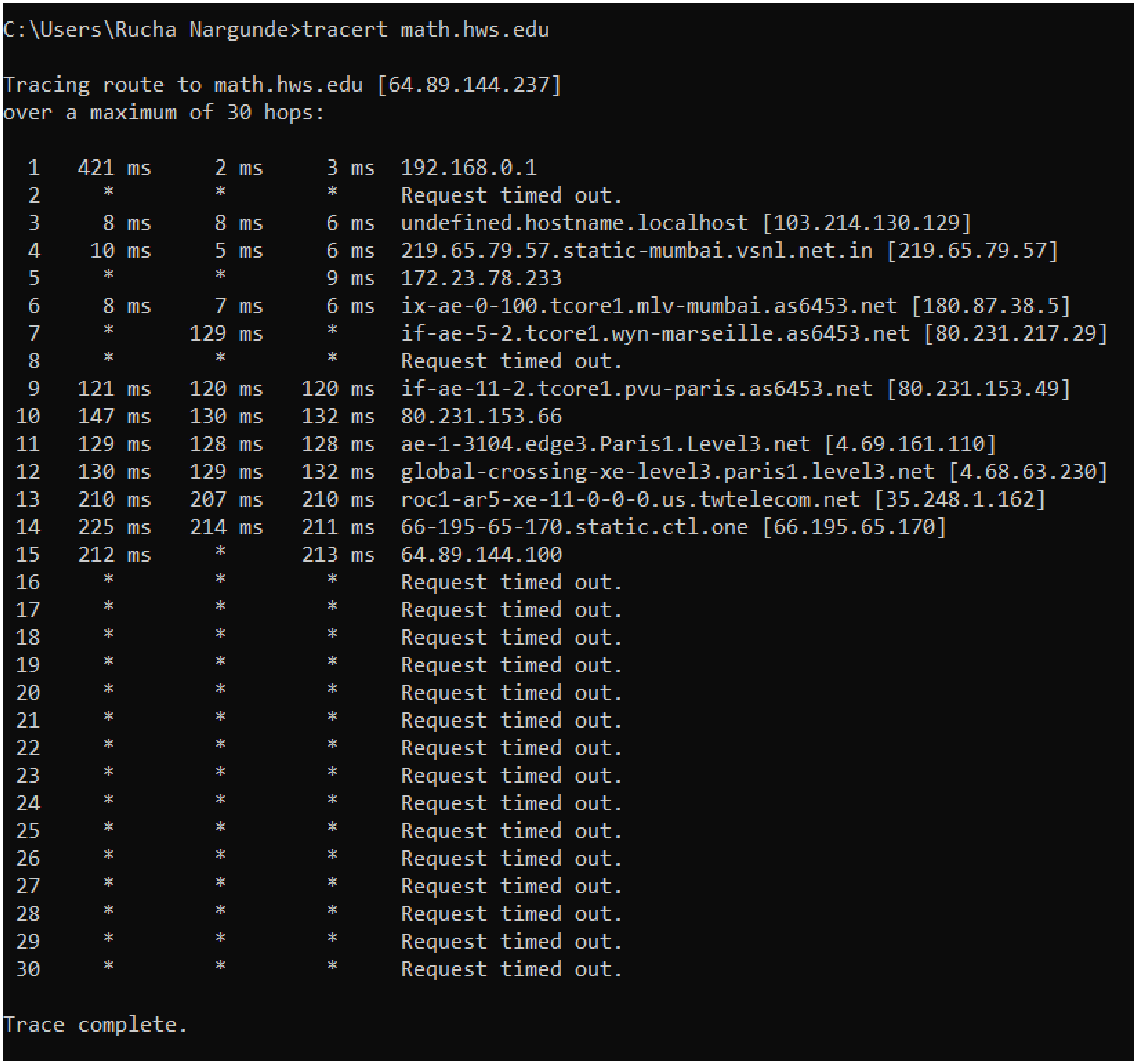
Exercise 2: (Very short.) Use traceroute to trace the route from your computer to math.hws.edu and to www.hws.edu. Explain the difference in the results.

Tracing route to www.hws.edu



```
C:\Users\Rucha Nargunde>tracert www.hws.edu

Tracing route to www.hws.edu [64.89.145.159]
over a maximum of 30 hops:

  1     3 ms     4 ms     2 ms  192.168.0.1
  2     *        *        6 ms  103.88.221.177
  3     5 ms     4 ms     5 ms  undefined.hostname.localhost [103.214.130.129]
  4     9 ms     6 ms     5 ms  219.65.79.57.static-mumbai.vsnl.net.in [219.65.79.57]
  5     *        7 ms     7 ms  172.23.78.233
  6     7 ms     9 ms     9 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7     *        *        *     Request timed out.
  8     *        *        *     Request timed out.
  9   121 ms     *      122 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *        *     Request timed out.
 11   131 ms   137 ms   139 ms  ae-2-3204.edge3.Paris1.Level3.net [4.69.161.114]
 12   134 ms   148 ms   129 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 13   211 ms   221 ms   208 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 14   215 ms   211 ms   211 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 15   221 ms   213 ms   213 ms  64.89.144.100
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

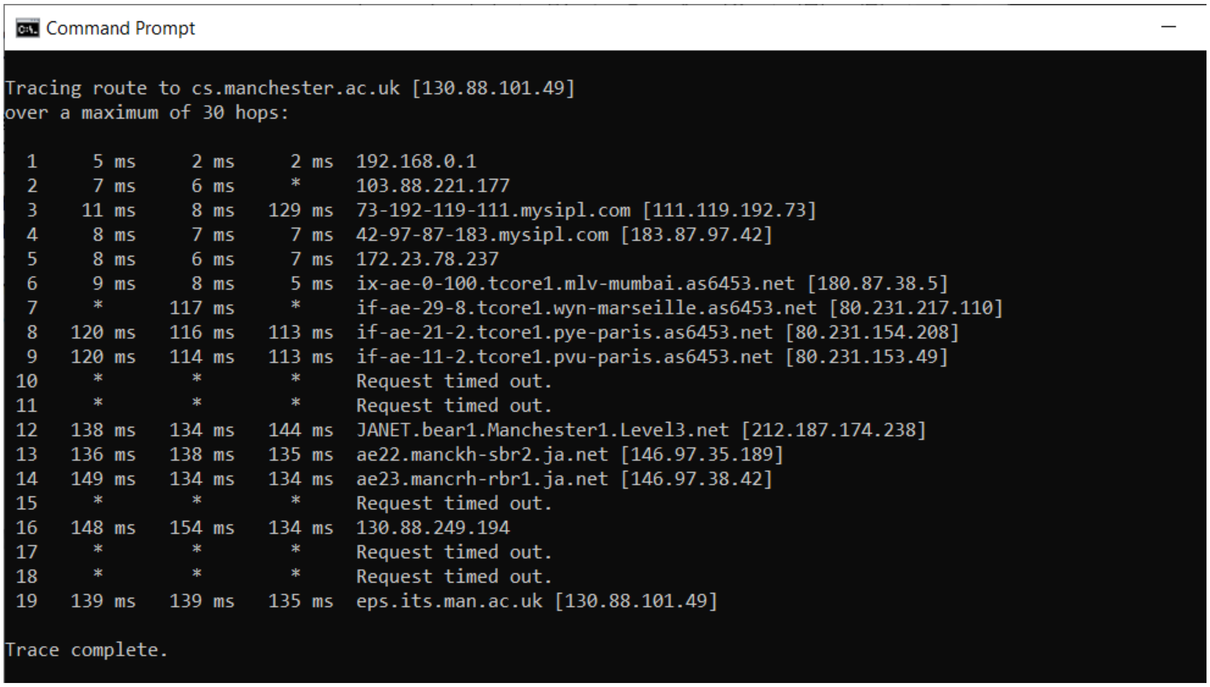
Tracing route to math.hws.edu



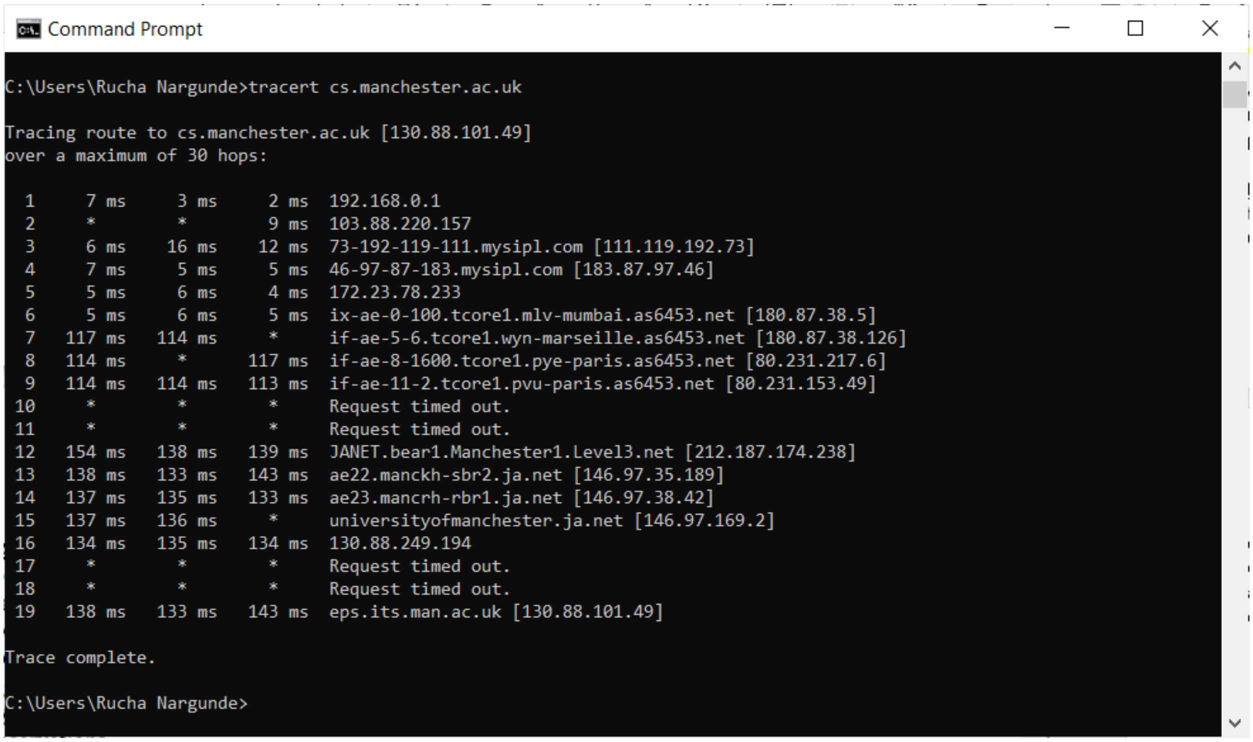
```
C:\Users\Rucha Nargunde>tracert math.hws.edu

Tracing route to math.hws.edu [64.89.144.237]
over a maximum of 30 hops:

  1   421 ms     2 ms     3 ms  192.168.0.1
  2     *        *        *     Request timed out.
  3     8 ms     8 ms     6 ms  undefined.hostname.localhost [103.214.130.129]
  4    10 ms     5 ms     6 ms  219.65.79.57.static-mumbai.vsnl.net.in [219.65.79.57]
  5     *        *        9 ms  172.23.78.233
  6     8 ms     7 ms     6 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7     *      129 ms     *     if-ae-5-2.tcore1.wyn-marseille.as6453.net [80.231.217.29]
  8     *        *        *     Request timed out.
  9   121 ms   120 ms   120 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10   147 ms   130 ms   132 ms  80.231.153.66
 11   129 ms   128 ms   128 ms  ae-1-3104.edge3.Paris1.Level3.net [4.69.161.110]
 12   130 ms   129 ms   132 ms  global-crossing-xe-level3.paris1.level3.net [4.68.63.230]
 13   210 ms   207 ms   210 ms  roc1-ar5-xe-11-0-0-0.us.twtelecom.net [35.248.1.162]
 14   225 ms   214 ms   211 ms  66-195-65-170.static.ctl.one [66.195.65.170]
 15   212 ms     *      213 ms  64.89.144.100
 16     *        *        *     Request timed out.
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19     *        *        *     Request timed out.
 20     *        *        *     Request timed out.
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
 23     *        *        *     Request timed out.
 24     *        *        *     Request timed out.
 25     *        *        *     Request timed out.
 26     *        *        *     Request timed out.
 27     *        *        *     Request timed out.
 28     *        *        *     Request timed out.
 29     *        *        *     Request timed out.
 30     *        *        *     Request timed out.

Trace complete.
```

As seen from the above screenshots, the IP address of the 2 destinations is slightly different. Also another observation is that no requests are responded to after the node 64.89.144.100.This is because the nodes beyond 64.89.144.100 do not respond to ICMP packets sent by the source.

Exercise 3: Two packets sent from the same source to the same destination do not necessarily follow the same path through the net. Experiment with some sources that are fairly far away. Can you find cases where packets sent to the same destination follow different paths? How likely does it seem to be? What about when the packets are sent at very different times? Save some of the outputs from traceroute. (You can copy them from the Terminal window by highlighting and right-clicking, then paste into a text editor.) Come back sometime next week and note your observations.



```
Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     5 ms     2 ms     2 ms  192.168.0.1
  2     7 ms     6 ms     *     103.88.221.177
  3    11 ms     8 ms   129 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4     8 ms     7 ms     7 ms  42-97-87-183.mysipl.com [183.87.97.42]
  5     8 ms     6 ms     7 ms  172.23.78.237
  6     9 ms     8 ms     5 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7     *      117 ms     *     if-ae-29-8.tcore1.wyn-marseille.as6453.net [80.231.217.110]
  8   120 ms   116 ms   113 ms  if-ae-21-2.tcore1.pye-paris.as6453.net [80.231.154.208]
  9   120 ms   114 ms   113 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   138 ms   134 ms   144 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 13   136 ms   138 ms   135 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 14   149 ms   134 ms   134 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 15     *        *        *     Request timed out.
 16   148 ms   154 ms   134 ms  130.88.249.194
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19   139 ms   139 ms   135 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.
```



```
C:\Users\Rucha Nargunde>tracert cs.manchester.ac.uk

Tracing route to cs.manchester.ac.uk [130.88.101.49]
over a maximum of 30 hops:

  1     7 ms     3 ms     2 ms  192.168.0.1
  2     *        *        9 ms  103.88.220.157
  3     6 ms    16 ms    12 ms  73-192-119-111.mysipl.com [111.119.192.73]
  4     7 ms     5 ms     5 ms  46-97-87-183.mysipl.com [183.87.97.46]
  5     5 ms     6 ms     4 ms  172.23.78.233
  6     5 ms     6 ms     5 ms  ix-ae-0-100.tcore1.mlv-mumbai.as6453.net [180.87.38.5]
  7   117 ms   114 ms     *     if-ae-5-6.tcore1.wyn-marseille.as6453.net [180.87.38.126]
  8   114 ms     *      117 ms  if-ae-8-1600.tcore1.pye-paris.as6453.net [80.231.217.6]
  9   114 ms   114 ms   113 ms  if-ae-11-2.tcore1.pvu-paris.as6453.net [80.231.153.49]
 10     *        *        *     Request timed out.
 11     *        *        *     Request timed out.
 12   154 ms   138 ms   139 ms  JANET.bear1.Manchester1.Level3.net [212.187.174.238]
 13   138 ms   133 ms   143 ms  ae22.manckh-sbr2.ja.net [146.97.35.189]
 14   137 ms   135 ms   133 ms  ae23.mancrh-rbr1.ja.net [146.97.38.42]
 15   137 ms   136 ms     *     universityofmanchester.ja.net [146.97.169.2]
 16   134 ms   135 ms   134 ms  130.88.249.194
 17     *        *        *     Request timed out.
 18     *        *        *     Request timed out.
 19   138 ms   133 ms   143 ms  eps.its.man.ac.uk [130.88.101.49]

Trace complete.

C:\Users\Rucha Nargunde>
```

From the screenshots shown above we can infer that although the source and destination is the same, it is not necessary that the same path will be traced every time. Although the initial nodes may be same, the intermediate nodes can change.

QUESTIONS ABOUT PATHS

Now look at the results you gathered and answer the following questions about the paths taken by your packets. Store your answers in a file named traceroute.txt.

1. Is any part of the path common for all hosts you tracerouted?

   Answer: Yes, in every path the first hop is always made to 192.168.0.1 which is the default gateway used by many wireless home routers. In many cases while tracing the route to international sites like www.hws.edu or www.cs.manchester.ac.uk , the second hop is also found to be common to 103.88.201.177

2. Is there a relationship between the number of nodes that show up in the traceroute and the location of the host? If so, what is this relationship?

   Answer: There is no relationship. Irrespective of the location, we are able to trace the route in a default number of 30 hops.

3. Is there a relationship between the number of nodes that show up in the traceroute and latency of the host (from your ping results above)? Does the same relationship hold for all hosts?

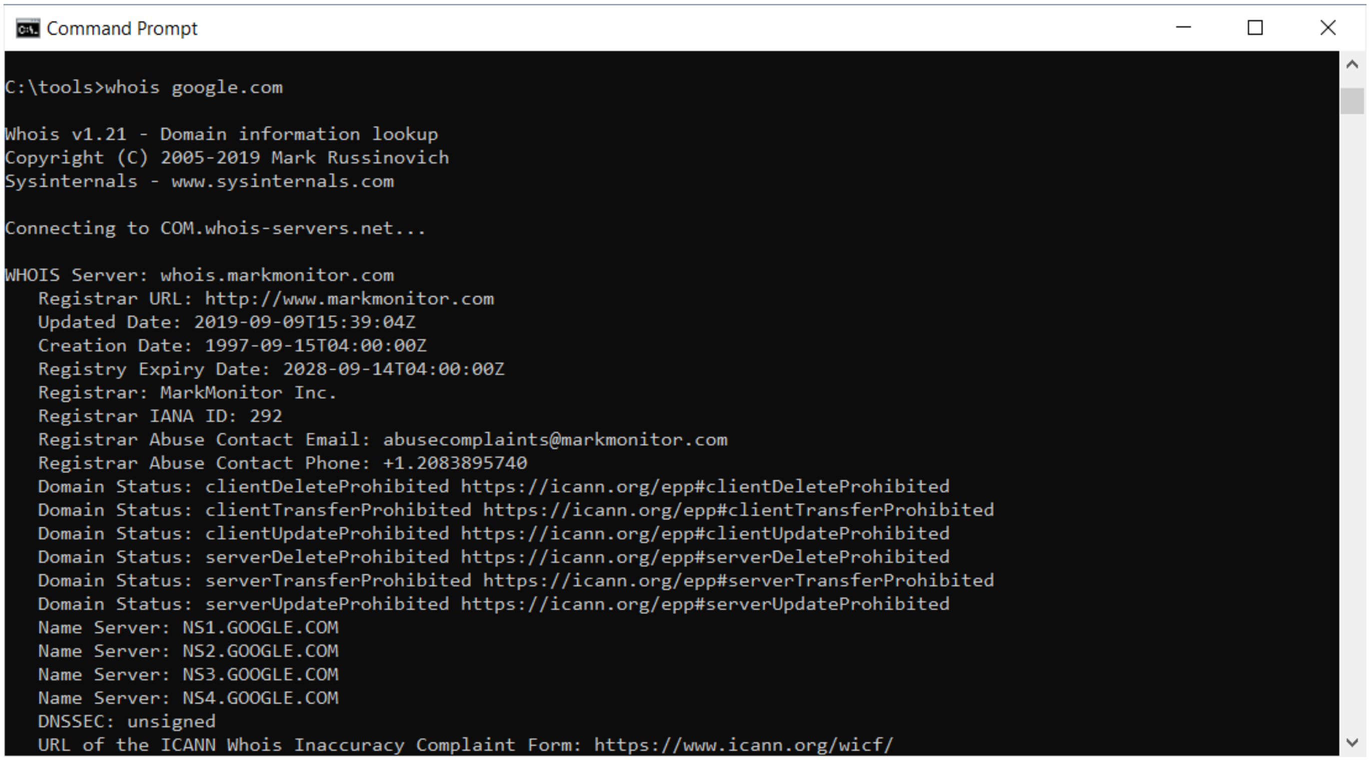
   Answer: There is no such relationship.

Whois — The whois command can give detailed information about domain names and IP addresses. If it is not installed on the computers then install it with command sudo apt-get install whois in. Whois can tell you what organization owns or is responsible for the name or address and where to contact them. It often includes a list of domain name servers for the organization.

When using whois to look up a domain name, use the simple two-part network name, not an individual computer name (for example, whois spit.ac.in).

Exercise 4: (Short.) Use whois to investigate a well-known web site such as google.com or amazon.com, and write a couple of sentences about what you find out.

To run whois command on windows we first have to download the whois utility from https://docs.microsoft.com/en-us/sysinternals/downloads/whois and them run the necessary command as shown in the screenshot below



```
C:\tools>whois google.com

Whois v1.21 - Domain information lookup
Copyright (C) 2005-2019 Mark Russinovich
Sysinternals - www.sysinternals.com

Connecting to COM.whois-servers.net...

WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

A whois record contains all the contact information associated with the person, company, or other entity that registered the domain name. A typical whois record will contain the following information [7]:

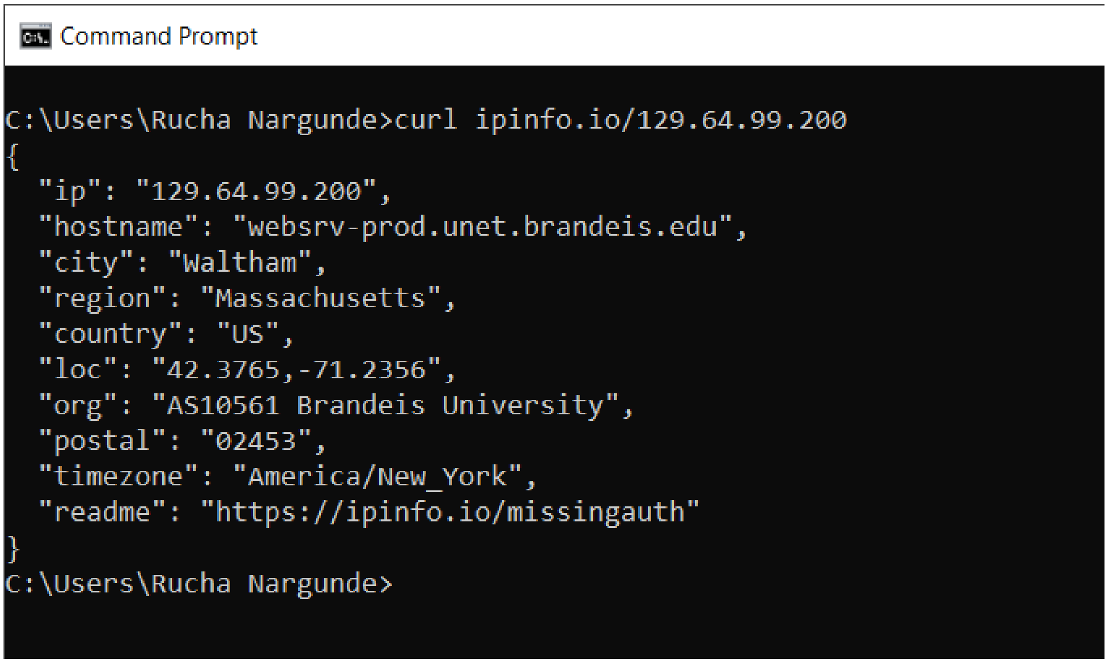
- **The name and contact information of the registrant:** The owner of the domain.
- **The name and contact information of the registrar:** The organization that registered the domain name.
- **The registration date.**
- **When the information was last updated.**
- **The expiration date.**

Exercise 5: (Should be short.) Because of NAT, the domain name spit.ac.in has a different IP address outside of SPIT than it does on campus. Using information in this lab and working on a home computer, find the outside IP address for spit.ac.in. Explain how you did it.

Geolocation — A geolocation service tries to tell, approximately, where a given IP address is located physically. They can't be completely accurate—but they probably get at least the country right most of the time.

This geolocation program is not installed on our computers, but you can access one on the command line using the curl command, which can send HTTP requests and display the response. The following command uses curl to contact a public web service that will look up an IP address for you: curl ipinfo.io/<IP-address>. For a specific example:

curl ipinfo.io/129.64.99.200



```
C:\Users\Rucha Nargunde>curl ipinfo.io/129.64.99.200
{
  "ip": "129.64.99.200",
  "hostname": "websrv-prod.unet.brandeis.edu",
  "city": "Waltham",
  "region": "Massachusetts",
  "country": "US",
  "loc": "42.3765,-71.2356",
  "org": "AS10561 Brandeis University",
  "postal": "02453",
  "timezone": "America/New_York",
  "readme": "https://ipinfo.io/missingauth"
}
C:\Users\Rucha Nargunde>
```

(As you can see, you get back more than just the location.)

Exercise 6: Find a few IP addresses that are connected to the web server on spit.ac.in right now, and determine where those IP addresses are located. (I'm expecting that there will be several; if not, try again in a few minutes or sometime later.) Find one that is far from Geneva, NY. Explain how you did it.

Conclusion:

- Through this experiment I have learned various command line utilities like ping, traceroute, pconfig that provide detailed information about the device and the quality of the network to which the device is connected.
- I also understood the difference between ping and traceroute commands. While ping is a quick and easy utility to tell if the specified server is live and reachable, traceroute finds the exact route taken to reach the server and time taken by each step (hop)

References:

1. https://www.geeksforgeeks.org/packet-switching-and-delays-in-computer-network/
2. https://www.callstats.io/blog/what-is-round-trip-time-and-how-does-it-relate-to-network-latency
3. https://searchnetworking.techtarget.com/
4. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat
5. https://help.fasthosts.co.uk/app/answers/detail/a_id/1550/~/traceroute-explained
6. https://www.inmotionhosting.com/support/website/ssh/read-traceroute/
7. https://www.howtogeek.com/680086/how-to-use-the-whois-command-on-linux/